

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-352322

(P2001-352322A)

(43) 公開日 平成13年12月21日 (2001. 12. 21)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード <sup>*</sup> (参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 1 1 B 20/10	H 5 C 0 5 3
G 1 1 B 20/10		H 0 4 L 9/00	6 0 1 A 5 D 0 4 4
H 0 4 N 5/91			6 0 1 D 5 J 1 0 4
			6 0 1 E

審査請求 未請求 請求項の数58 O L (全 70 頁) 最終頁に続く

(21) 出願番号 特願2000-243205(P2000-243205)

(22) 出願日 平成12年 8 月10日 (2000. 8. 10)

(31) 優先権主張番号 特願2000-105328(P2000-105328)

(32) 優先日 平成12年 4 月 6 日 (2000. 4. 6)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川 6 丁目 7 番35号

(72) 発明者 浅野 智之

東京都品川区北品川 6 丁目 7 番35号 ソニ  
ー株式会社内

(72) 発明者 大澤 義知

東京都品川区北品川 6 丁目 7 番35号 ソニ  
ー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外 2 名)

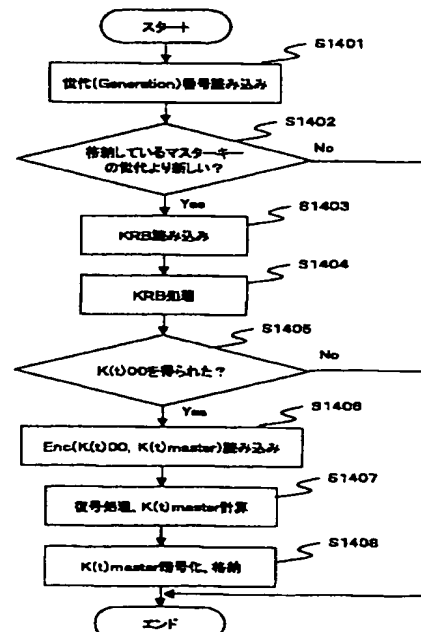
最終頁に続く

(54) 【発明の名称】 情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57) 【要約】

【課題】 ツリー (木) 構造の鍵配布構成によりキーの配布を実行して、効率的な鍵更新処理を可能とする。

【解決手段】 ツリー構造の鍵配布構成により、マスターキー、メディアキーの更新をキー更新ブロック (K R B) とともに送信する。K R B は、ツリーのリーフを構成するデバイスにリーフキーおよび限定したノードキーを保有させた構成であり、特定のノードにより特定されるグループに特定のキー更新ブロック (K R B) を生成して配布して、更新可能デバイスを限定することができる。グループに属さないデバイスは復号できず、キー配信の安全性が確保される。特に、世代管理を行なったマスターキーを使用するシステムにおいて、K R B による更新マスターキーを配布する構成が実現される。



## 【特許請求の範囲】

【請求項1】記録媒体に情報を記録する情報記録装置において、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

記録媒体に対する格納データの暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記情報記録装置に内蔵した暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号化処理を実行する構成を有し、

前記暗号化キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報記録装置。

【請求項2】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項1に記載の情報記録装置。

【請求項3】前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項1に記載の情報記録装置。

【請求項4】前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記暗号化キー生成用データの更新データを受領し、

キー更新ブロック(KRB)の暗号化処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項5】前記キー更新ブロック(KRB)は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック(KRB)についての暗号化処理を実行する構成であることを特徴とする請求項4に記載の情報記録装置。

【請求項6】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理手段は、

前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項7】前記情報記録装置は、さらに、

第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、

前記情報記録装置に内蔵した第2の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第2の暗号化キーを生成して該第2の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、

を選択的に実行する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項8】前記暗号処理手段は、

前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の暗号化キーを生成し、

前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の暗号化キーを生成する構成であることを特徴とする請求項7に記載の情報記録装置。

【請求項9】前記情報記録装置は、さらに、

間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理手段を有し、

前記暗号処理手段は、

前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、

前記記録媒体に対する格納データの暗号化処理においては、前記暗号化キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項10】前記暗号処理手段は、

前記記録媒体に対する格納データの暗号化処理をDESアルゴリズムに従って実行する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項11】前記情報記録装置は、

記録媒体に対する記録対象となる情報を受信するインタ

フェース手段を有し、

前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各バケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項12】前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項13】記録媒体から情報を再生する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を実行する暗号処理手段を有し、前記暗号処理手段は、前記情報記録装置に内蔵した復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する構成を有し、前記復号キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかを有して更新可能なデータとして構成されていることを特徴とする情報再生装置。

【請求項14】前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項13に記載の情報再生装置。

【請求項15】前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項13に記載の情報再生装置。

【請求項16】前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記復号キー生成用データの更新データを受領し、キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項17】前記キー更新ブロック(KRB)は、記

録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック(KRB)についての暗号処理を実行する構成であることを特徴とする請求項16に記載の情報再生装置。

【請求項18】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項19】前記情報再生装置は、さらに、前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第2の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第2の復号キーを生成して該第2の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、を選択的に実行する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項20】前記暗号処理手段は、

前記再生機器制限なしの復号処理において、情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、

記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーと、暗号データを記録した情報記録装置の識別子であるデバイスID情報記録装置の識別子であるデバイスIDとを取得し、

前記マスターキー、ディスクID、タイトルキー、デバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の復号キーを生成し、

前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、

情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、

記録媒体から、記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクID、タイトルキー、デバ

イス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の復号キーを生成する構成であることを特徴とする請求項19に記載の情報再生装置。

【請求項21】前記情報再生装置は、前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ATS）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ATS）の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成する構成を有し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項22】前記暗号処理手段は、前記記録媒体に格納された暗号データの復号処理をDESアルゴリズムに従って実行する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項23】前記情報再生装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項24】前記情報再生装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI（Encryption Mode Indicator）を識別し、該EMIに基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項25】記録媒体に情報を記録する情報記録方法において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に

格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とする情報記録方法。

【請求項26】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項25に記載の情報記録方法。

【請求項27】前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項25に記載の情報記録方法。

【請求項28】前記情報記録方法において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（KRB）を更新対象となるリーフの情報記録装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック（KRB）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする請求項25に記載の情報記録方法。

【請求項29】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、さらに、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求項25に記載の情報記録方法。

【請求項30】前記暗号処理ステップは、第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、前記情報記録装置に内蔵した第2の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第2の暗号化キーを生成して該第2の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、を選択的に実行することを特徴とする請求項25に記載の情報記録方法。

【請求項31】前記暗号処理ステップは、前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報

記録装置の識別子であるデバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の暗号化キーを生成し、前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の暗号化キーを生成する構成であることを特徴とする請求項30に記載の情報記録方法。

【請求項32】前記情報記録方法は、さらに、間欠的なトランスポートバケットから成るトランスポートストリームを構成する各バケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報(ATS)の付加された1以上のバケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成し、前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする請求項25に記載の情報記録方法。

【請求項33】前記暗号処理ステップは、前記記録媒体に対する格納データの暗号処理をDESアルゴリズムに従って実行することを特徴とする請求項25に記載の情報記録方法。

【請求項34】前記情報記録方法は、さらに、データを構成するトランスポートストリームに含まれる各バケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御することを特徴とする請求項25に記載の情報記録方法。

【請求項35】前記情報記録方法は、さらに、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御することを特徴とする請求項25に記載の情報記録方法。

【請求項36】記録媒体から情報を再生する情報再生方法であり、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とする情報再生方法。

【請求項37】前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項36に記載の情報再生方法。

【請求項38】前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項36に記載の情報再生方法。

【請求項39】前記情報再生方法において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする請求項36に記載の情報再生方法。

【請求項40】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成することを特徴とする請求項36に記載の情報再生方法。

【請求項41】前記情報再生方法は、さらに、前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第2の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第2の復号キーを生成して該第2の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、を選択的に実行することを特徴とする請求項36に記載の情報再生方法。

【請求項42】前記復号処理ステップは、前記再生機器制限なしの復号処理において、

情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーと、暗号データを記録した情報記録装置の識別子であるデバイスID情報記録装置の識別子であるデバイスIDとを取得し、前記マスターキー、ディスクID、タイトルキー、デバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の復号キーを生成し、前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクID、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の復号キーを生成することを特徴とする請求項41に記載の情報再生方法。

【請求項43】前記情報再生方法において、情報再生装置は、復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ATS）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記復号処理ステップは、前記受信時刻情報（ATS）の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする請求項36に記載の情報再生方法。

【請求項44】前記復号処理ステップは、前記記録媒体に格納された暗号データの復号処理をDESアルゴリズムに従って実行することを特徴とする請求項36に記載の情報再生方法。

【請求項45】前記情報再生方法は、さらに、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする請求項36に記載の情報再生方法。

【請求項46】前記情報再生方法は、さらに、コピーを制御するためのコピー制御情報としての2ビットのEMI（Encryption Mode Indicator）を識別し、該EMIに基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする請求項36に記載の情報再生方法。

【請求項47】情報を記録可能な情報記録媒体であって、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（KRB）を格納したことを特徴とする情報記録媒体。

【請求項48】前記情報記録媒体は、さらに、情報記録装置において記録媒体に格納するデータの暗号化処理に用いる暗号化キーを生成するための暗号化キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする請求項47に記載の情報記録媒体。

【請求項49】前記情報記録媒体は、さらに、情報再生装置において記録媒体に格納された暗号データの復号処理に用いる復号キーを生成するための復号キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする請求項47に記載の情報記録媒体。

【請求項50】前記情報記録媒体は、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納した構成であることを特徴とする請求項47に記載の情報記録媒体。

【請求項51】情報記録媒体を製造する記録媒体製造装置であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（KRB）を格納するメモリと、前記メモリに格納されたキー更新ブロック（KRB）の前記記録媒体に対する書き込み制御を実行する制御部と、を有することを特徴とする記録媒体製造装置。

【請求項52】前記メモリには、さらに、記録媒体識別子と、暗号化された暗号化キー生成用データまたは暗号化された復号キー生成用データの少なくともいずれかを格納し、前記制御部は、前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込み制御を実行する構成であることを特徴

とする請求項51に記載の記録媒体製造装置。

【請求項53】前記メモリには、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする請求項51に記載の記録媒体製造装置。

【請求項54】記録媒体を製造する記録媒体製造方法であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)をメモリに格納するステップと、前記メモリに格納されたキー更新ブロック(KRB)の前記記録媒体に対する書き込みを実行するステップと、を有することを特徴とする記録媒体製造方法。

【請求項55】前記記録媒体製造方法において、前記メモリに、さらに、記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかを格納し、前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込みを実行することを特徴とする請求項54に記載の記録媒体製造方法。

【請求項56】前記記録媒体製造方法において、前記メモリに、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込みを実行することを特徴とする請求項54に記載の記録媒体製造方法。

【請求項57】記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体。

【請求項58】記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく抑えて、マスターキーあるいはメディアキー等の鍵更新におけるデータ配信の負荷を軽減することを可能とした構成を提供する。具体的には、各記録再生器機器をn分木の各葉(リーフ)に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵(マスターキーもしくはメディアキー)を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み(システム)が導入されている。

【0003】例えば、MD(ミニディスク)(MDは商標)装置において、違法なコピーを防止する方法として、SCMS(Serial Copy Management System)が採用

されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース(DIF)から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0004】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー(copy free)のデータであるか、1度だけコピーが許されている(copy once allowed)データであるか、またはコピーが禁止されている(copy prohibited)データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー(copy free)となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可(copy once allowed)となっている場合には、SCMS信号をコピー禁止(copy prohibited)に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止(copy prohibited)となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっていく。

【0005】しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【0006】コンテンツ・スクランブルシステムでは、DVD-ROM(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー(復号鍵)が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0007】一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化

データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっていく。

【0008】しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体(以下、適宜、ROMメディアという)を対象としており、ユーザによるデータの書き込みが可能な記録媒体(以下、適宜、RAMメディアという)への適用については考慮されていない。

【0009】即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0010】そこで、本出願人は、先の特許出願、特開平11-224461号公報(特願平10-25310号)において、個々の記録媒体を識別する為の情報(以下、媒体識別情報と記述する)を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0011】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー(マスターキー)により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製(違法コピー)ができないように、その動作が規定される。

【0012】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【0013】

【発明が解決しようとする課題】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他



の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【0014】しかし、この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【0015】本発明は、上述の問題点を解決することを目的とするものであり、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく抑え、新たな更新キーの配信の負荷を軽減することを可能とした構成を提供する。すなわち、各機器を $n$ 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する格納データの暗号化処理を実行する暗号処理手段を有し、前記暗号処理手段は、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する構成を有し、前記暗号化キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報記録装置にある。

【0017】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

【0018】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【0019】さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（KRB）を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記暗号化キー生成用データの更新データを受領し、キー更新ブロック（KRB）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する構成を有することを特徴とする。

【0020】さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック（KRB）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（KRB）についての暗号処理を実行する構成であることを特徴とする。

【0021】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理手段は、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【0022】さらに、本発明の情報記録装置の一実施態様において、第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、前記情報記録装置に内蔵した第2の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第2の暗号化キーを生成して該第2の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、を選択的に実行する構成を有することを特徴とする。

【0023】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の暗号化キーを生成し、前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイト

ルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の暗号化キーを生成する構成であることを特徴とする。

【0024】さらに、本発明の情報記録装置の一実施態様において、間欠的なトランスポートバケットから成るトランスポートストリームを構成する各バケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報(ATS)の付加された1以上のバケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする。

【0025】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記記録媒体に対する格納データの暗号処理をDESアルゴリズムに従って実行する構成であることを特徴とする。

【0026】さらに、本発明の情報記録装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各バケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

【0027】さらに、本発明の情報記録装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

【0028】さらに、本発明の第2の側面は、記録媒体から情報を再生する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を実行する暗号処理手段を有し、前記暗号処理手段は、前記情報記録装置に内蔵した復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する構成を有し、前記復号キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかをを用いて更新可能なデータとして構成されていることを特徴とする情報再生装置にある。

【0029】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報

記録装置において共通なマスターキーであることを特徴とする。

【0030】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【0031】さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含みキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記復号キー生成用データの更新データを受領し、キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する構成を有することを特徴とする。

【0032】さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック(KRB)は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック(KRB)についての暗号処理を実行する構成であることを特徴とする。

【0033】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成する構成であることを特徴とする。

【0034】さらに、本発明の情報再生装置の一実施態様において、前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第2の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第2の復号キーを生成して該第2の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、を選択的に実行する構成を有することを特徴とする。

【0035】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記再生機器制限なしの復号処理において、情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーと、暗号デ

ータを記録した情報記録装置の識別子であるデバイスID情報記録装置の識別子であるデバイスIDとを取得し、前記マスターキー、ディスクID、タイトルキー、デバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の復号キーを生成し、前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクID、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の復号キーを生成する構成であることを特徴とする。

【0036】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成する構成を有し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする。

【0037】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号データの復号処理をDESアルゴリズムに従って実行する構成であることを特徴とする。

【0038】さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする。

【0039】さらに、本発明の情報再生装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする。

【0040】さらに、本発明の第3の側面は、記録媒体に情報を記録する情報記録方法において、複数の異なる

情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号化処理を実行する暗号化処理ステップと、を有することを特徴とする情報記録方法にある。

【0041】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

【0042】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【0043】さらに、本発明の情報記録方法の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報記録装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック(KRB)の暗号化処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

【0044】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号化処理ステップは、さらに、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【0045】さらに、本発明の情報記録方法の一実施態様において、前記暗号化処理ステップは、第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号化処理と、前記情報記録装置に内蔵した第2の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第2の暗号化キーを生成して該第2の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号化処理と、を選択的に実行することを特徴とする。

【0046】さらに、本発明の情報記録方法の一実施態

様において、前記暗号処理ステップは、前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の暗号化キーを生成し、前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の暗号化キーを生成する構成であることを特徴とする。

【0047】さらに、本発明の情報記録方法の一実施態様において、間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成し、前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする。

【0048】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記記録媒体に対する格納データの暗号処理をDESアルゴリズムに従って実行することを特徴とする。

【0049】さらに、本発明の情報記録方法の一実施態様において、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御することを特徴とする。

【0050】さらに、本発明の情報記録方法の一実施態様において、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御することを特徴とする。

【0051】さらに、本発明の第4の側面は、記録媒体から情報を再生する情報再生方法であり、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された

復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とする情報再生方法にある。

【0052】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

【0053】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【0054】さらに、本発明の情報再生方法の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

【0055】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成することを特徴とする。

【0056】さらに、本発明の情報再生方法の一実施態様において、前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第2の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第2の復号キーを生成して該第2の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、を選択的に実行することを特徴とする。

【0057】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記再生機器制限なしの復号処理において、情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーと、暗号データを記録した情報記録装置の識別子であるデバイ

スID情報記録装置の識別子であるデバイスIDとを取得し、前記マスターキー、ディスクID、タイトルキー、デバイスIDとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第1の復号キーを生成し、前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクIDと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクID、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第2の復号キーを生成することを特徴とする。

【0058】さらに、本発明の情報再生方法の一実施態様において、情報再生装置は、復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記復号処理ステップは、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする。

【0059】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記記録媒体に格納された暗号データの復号処理をDESアルゴリズムに従って実行することを特徴とする。

【0060】さらに、本発明の情報再生方法の一実施態様において、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする。

【0061】さらに、本発明の情報再生方法の一実施態様において、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする。

【0062】さらに、本発明の第5の側面は、情報を記録可能な情報記録媒体であって、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を格納したことを特徴とする情報記録媒体にある。

【0063】さらに、本発明の情報記録媒体の一実施態様において、情報記録装置において記録媒体に格納するデータの暗号化処理に用いる暗号化キーを生成するための暗号化キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする。

【0064】さらに、本発明の情報記録媒体の一実施態様において、情報再生装置において記録媒体に格納された暗号データの復号処理に用いる復号キーを生成するための復号キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする。

【0065】さらに、本発明の情報記録媒体の一実施態様において、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納した構成であることを特徴とする。

【0066】さらに、本発明の第6の側面は、情報記録媒体を製造する記録媒体製造装置であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を格納するメモリと、前記メモリに格納されたキー更新ブロック(KRB)の前記記録媒体に対する書き込み制御を実行する制御部と、を有することを特徴とする記録媒体製造装置にある。

【0067】さらに、本発明の記録媒体製造装置の一実施態様において、前記メモリには、さらに、記録媒体識別子と、暗号化された暗号化キー生成用データまたは暗号化された復号キー生成用データの少なくともいずれかを格納し、前記制御部は、前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする。

【0068】さらに、本発明の記録媒体製造装置の一実施態様において、前記メモリには、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする。

【0069】さらに、本発明の第7の側面は、記録媒体を製造する記録媒体製造方法であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)をメモリに格納するステップと、前記メモリに格納されたキー更新ブロック(KRB)の前記記録媒体に対する書き込みを実行するステップと、を有することを特徴とする記録媒体

製造方法にある。

【0070】さらに、本発明の記録媒体製造方法の一実施態様において、前記メモリに、さらに、記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかを格納し、前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込みを実行することを特徴とする。

【0071】さらに、本発明の記録媒体製造方法の一実施態様において、前記記録媒体製造方法において、前記メモリに、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込みを実行することを特徴とする。

【0072】さらに、本発明の第8の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかをを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0073】さらに、本発明の第9の側面は、記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかをを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0074】

【作用】本発明の構成においては、ツリー（木）構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく抑えている。すなわち、各機器をn分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コン

テンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。

【0075】また、本発明の1つの態様としては、記録媒体に記録するコンテンツの形式をMPEG2 TSパケット（packet）とし、このパケットを記録装置が受信した時刻情報であるATSを付加して記録する。ATSは24乃至32ビットのデータであり、ある程度のランダム性がある。ここで、ATSはArrival Time Stamp（着信時刻スタンプ）の略である。記録媒体のひとつのブロック（セクタ）には、ATSを付加したTSパケットをX個記録することにし、その第1番目のTSパケットに付加されたATSを用いてそのブロックのデータを暗号化するブロックキーを生成する。

【0076】このようにすることにより、各ブロックごとに固有の鍵を用いて暗号化することができ、また鍵を格納する特別な領域も不要となり、記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなる。

【0077】さらに、TSパケットにATSだけでなくコピー制限情報（CCI：Copy Control Information）も付加して記録し、ATSとCCIを用いてブロックキーを生成するようにすることも可能である。

【0078】なお、本発明の第8および第9の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0079】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0080】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0081】

【発明の実施の形態】〔システム構成〕図1は、本発明を適用した記録再生装置100の一実施例構成を示すブロック図である。記録再生装置100は、入出力I/F（Interface）120、MPEG（Moving Picture Experts Group）コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F（Interface）140、暗号

処理手段150、ROM (Read Only Memory) 160、CPU (Central Processing Unit) 170、メモリ180、記録媒体195のドライブ190、さらにトランスポート・ストリーム処理手段 (TS処理手段) 300を有し、これらはバス110によって相互に接続されている。

【0082】入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D (Analog Digital) 変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

【0083】暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated Circuit) で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0084】ROM160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。CPU170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し (再生し)、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。また、プログラムをROM160に、デバイスキーをメモリ180に記録する構成としてもよい。

【0085】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0086】トランスポート・ストリーム処理手段 (TS処理手段) 300は、後段において図6以下を用いて詳細に説明するが、例えば複数のTVプログラム (コンテンツ) が多重化されたトランスポートストリームから特定のプログラム (コンテンツ) に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体195に格納するためのデータ処理および、記録媒体195からの再生処理時の出現タイミング制御処理を行なう。

【0087】トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのATS (Arrival Time Stamp: 着信時刻スタンプ) が設定されており、このタイミングはMPEG2システムズで規定されている仮想的なデコーダであるTSTD (Transport stream System Target Decoder) を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたATSによって出現タイミングを制御する。トランスポート・ストリーム処理手段 (TS処理手段) 300は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段 (TS処理手段) 300は、DVD等の記録媒体195へのデータ記録時に、各トランスポートパケットの入力タイミングを表すATS (Arrival Time Stamp: 着信時刻スタンプ) を付加して記録する。

【0088】本発明の記録再生装置100は、上述のATSの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段150において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体195に格納する。さらに、暗号処理手段150は、記録媒体195に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

【0089】なお、図1に示す暗号処理手段150、TS処理手段300は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する1つのワンチップLSIとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によ

て実現する構成としてもよい。

【0090】本発明の記録再生装置の構成例としては図1に示す構成の他に図2に示す構成が可能である。図2に示す記録再生装置200では、記録媒体205はドライブ装置としての記録媒体インタフェース(I/F)210から着脱が可能であり、この記録媒体205を別の記録再生装置に装着してもデータの読出し、書きこみが可能な構成としたものである。

【0091】【データ記録処理およびデータ再生処理】次に、図1あるいは図2の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図3および図4のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体195に記録する場合においては、図3(A)のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ(デジタルコンテンツ)が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS301において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、TS処理手段300に出力する。

【0092】TS処理手段300は、ステップS302において、トランスポートストリームを構成する各トランスポートパケットにATSを付加したブロックデータを生成して、バス110を介して、暗号処理手段150に出力する。

【0093】暗号処理手段150は、ステップS303において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス110を介して、ドライブ190、あるいは記録媒体I/F210に出力する。暗号化コンテンツは、ドライブ190、あるいは記録媒体I/F210を介して記録媒体195に記録(S304)され、記録処理を終了する。なお、暗号処理手段150における暗号処理については後段で説明する。

【0094】なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するとき、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、SCDTC(Five Company Digital Transmission Content Protection)(以下、適宜、DTCPという)が定められているが、このDTCPでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ(暗号化コンテンツ)を復号するようになっている。

【0095】このDTCPに規格に基づくデータ送受信においては、データ受信側の入出力I/F120は、ステップS301で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DTCPに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段150に出力する。

【0096】DTCPによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0097】なお、DTCPによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、DTCPについては、例えば、<http://www.dtcp.com>のURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメーションバージョン(Informational Version)の取得が可能である。

【0098】次に、外部からのアナログ信号のコンテンツを、記録媒体195に記録する場合の処理について、図3(B)のフローチャートに従って説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS321において、そのアナログコンテンツを受信し、ステップS322に進み、内蔵するA/D、D/Aコンバータ141でA/D変換して、デジタル信号のコンテンツ(デジタルコンテンツ)とする。

【0099】このデジタルコンテンツは、MPEGコーデック130に供給され、ステップS323において、MPEGエンコード、すなわちMPEG圧縮による符号化処理が実行され、バス110を介して、暗号処理手段150に供給される。

【0100】以下、ステップS324、S325、S326において、図3(A)のステップS302、S303における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0101】次に、記録媒体195に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナ



ログコンテンツとして出力する処理について図4のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図4(A)のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップS401において、ドライブ190または記録媒体1/F210によって、記録媒体195に記録された暗号化コンテンツが読み出され、バス110を介して、暗号処理手段150に出力される。

【0102】暗号処理手段150では、ステップS402において、ドライブ190または記録媒体1/F210から供給される暗号化コンテンツが復号処理され、復号データがバス110を介して、TS処理手段300に出力される。

【0103】TS処理手段300は、ステップS403において、トランスポートストリームを構成する各トランスポートパケットのATSから出力タイミングを判定し、ATSに応じた制御を実行して、バス110を介して、入出力1/F120に供給する。入出力1/F120は、TS処理手段300からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、TS処理手段300の処理、暗号処理手段150におけるデジタルコンテンツの復号処理については後述する。

【0104】なお、入出力1/F120は、ステップS404で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、DTCIPの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【0105】記録媒体195に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図4(B)のフローチャートに従った再生処理が行われる。

【0106】即ち、ステップS421、S422、S423において、図4(A)のステップS401、S402、S403における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0107】MPEGコーデック130では、ステップS424において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力1/F140に供給される。入出力1/F140は、ステップS424において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S425)して、アナログコンテンツとする。そして、ステップS426に進み、入出力1/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【0108】【データフォーマット】次に、図5を用いて、本発明における記録媒体上のデータフォーマットを

説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。1ブロックは、 $192 \times X$  (エックス) バイト (例えば  $X=32$ ) の大きさとなっている。

【0109】本発明では、MPEG2のTS (トランスポート・ストリーム) パケット (188バイト) にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとしている。ATSは24乃至32ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp (着信時刻スタンプ) の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック (セクタ) には、ATSを付加したTS (トランスポート・ストリーム) パケットをX個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック (セクタ) のデータを暗号化するブロックキーを生成する。

【0110】ランダム性のあるATSを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【0111】なお、図5に示すブロック・シード (Block Seed) は、ATSを含む付加情報である。ブロック・シードは、さらにATSだけでなくコピー制限情報 (CCI: Copy Control Information) も付加した構成としてもよい。この場合、ATSとCCIを用いてブロックキーを生成する構成とすることができる。

【0112】なお、本発明の構成においては、DVD等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭のm (たとえば、 $m=8$  または16) バイトは暗号化されずに平文 (Unencrypted data) のまま記録され、残りのデータ ( $m+1$  バイト以降) が暗号化される。これは暗号処理が8バイト単位としての処理であるために暗号処理データ長 (Encrypted data) に制約が発生するためである。なお、もし、暗号処理が8バイト単位でなく、たとえば1バイト単位で行なえるなら、 $m=4$  として、ブロックシード以外の部分をすべて暗号化してもよい。

【0113】【TS処理手段における処理】ここで、ATSの機能について詳細に説明する。ATSは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するため

に付加する着信時刻スタンプである。

【0114】すなわち、例えば複数のTVプログラム(コンテンツ)が多重化されたトランスポートストリームの中から1つまたは幾つかのTVプログラム(コンテンツ)を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる(図7(a)参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはMPEG2システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるT-S T D (Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

【0115】トランスポートストリームの再生時には、各トランスポートパケットに付加されたATSによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要がある、トランスポートパケットをDVD等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すATSを付加して記録する。

【0116】図6に、デジタルインタフェース経由で入力されるトランスポートストリームをDVD等の記録媒体であるストレージメディアに記録する時のTS処理手段300において実行する処理を説明するブロック図を示す。端子600からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図1または図2においては、入出力1/F120を介して、あるいは入出力1/F140、MPEGコーデック130を介して端子600からトランスポートストリームが入力される。

【0117】トランスポートストリームは、ビットストリームパーサ(parser)602に入力される。ビットストリームパーサ602は、入力トランスポートストリームの中からPCR(Program Clock Reference)パケットを検出する。ここで、PCRパケットとは、MPEG2システムズで規定されているPCRが符号化されているパケットである。PCRパケットは、100msec以内の時間間隔で符号化されている。PCRは、トランスポートパケットが受信側に到着する時刻を27MHzの精度で表す。

【0118】そして、27MHzPLL603において、記録再生器が持つ27MHzクロックをトランスポートストリームのPCRにロック(Lock)させる。タイムスタンプ発生回路604は、27MHzクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード(Block seed)付加回路605は、トランスポートパケットの第1バイト目がスミージングバッファ606へ入力される時のタイムスタンプをATSとして、そのトランスポートパケットに付

加する。

【0119】ATSが付加されたトランスポートパケットは、スミージングバッファ606を通して、端子607から、暗号処理手段150に出力され、後段で説明する暗号処理が実行された後、ドライブ190(図1)、記録媒体1/F210(図2)を介してストレージメディアである記録媒体195に記録される。

【0120】図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図7(a)は、ある特定プログラム(コンテンツ)を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図7(a)に示すように不規則なタイミングで現れる。

【0121】図7(b)は、ブロック・シード(Block Seed)付加回路605の出力を示す。ブロック・シード(Block Seed)付加回路605は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すATSを含むブロック・シード(Block Seed)を付加して、ソースパケットを出力する。図7(c)は記録媒体に記録されたソースパケットを示す。ソースパケットは、図7(c)に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【0122】図8は、記録媒体195に記録されたトランスポートストリームを再生する場合のTS処理手段300の処理構成ブロック図を示している。端子800からは、後段で説明する暗号処理手段において復号されたATS付きのトランスポートパケットが、ブロック・シード(Block seed)分離回路801へ入力され、ATSとトランスポートパケットが分離される。タイミング発生回路804は、再生器が持つ27MHzクロック805のクロックカウンタ値に基づいた時間を計算する。

【0123】なお、再生の開始時において、一番最初のATSが初期値として、タイミング発生回路804にセットされる。比較器803は、ATSとタイミング発生回路804から入力される現在の時刻を比較する。そして、タイミング発生回路804が発生する時間とATSが等しくなった時、出力制御回路802は、そのトランスポートパケットをMPEGコーデック130またはデジタル入出力1/F120へ出力する。

【0124】図9は、入力AV信号を記録再生器100のMPEGコーデック130においてMPEGエンコードして、さらにTS処理手段300においてトランスポートストリームを符号化する構成を示す。従って図9は、図1または、図2におけるMPEGコーデック130とTS処理手段300の両処理構成を併せて示すブロック図である。端子901からは、ビデオ信号が入力されており、それはMPEGビデオエンコーダ902へ入力される。

【0125】MPEGビデオエンコーダ902は、入力ビデオ信号をMPEGビデオストリームに符号化し、それをバッファビデオストリームバッファ903へ出力する。また、MPEGビデオエンコーダ902は、MPEGビデオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/Bピクチャ (picture) の情報である。また、デコードタイムスタンプは、MPEG2システムズで規定されている情報である。

【0126】端子904からは、オーディオ信号が入力されており、それはMPEGオーディオエンコーダ905へ入力される。MPEGオーディオエンコーダ905は、入力オーディオ信号をMPEGオーディオストリームに符号化し、それをバッファ906へ出力する。また、MPEGオーディオエンコーダ905は、MPEGオーディオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

【0127】多重化スケジューラ908には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ908は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ908は、内部に27MHz精度の基準時刻を発生するクロックを持ち、そして、MPEG2で規定されている仮想的なデコーダモデルであるT-S-TDを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【0128】パケット符号化制御情報がビデオパケットの場合、スイッチ976はa側になり、ビデオストリームバッファ903からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0129】パケット符号化制御情報がオーディオパケットの場合、スイッチ976はb側になり、オーディオストリームバッファ906から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0130】パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込

み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

【0131】トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すATSを計算する。

【0132】多重化スケジューラ908から入力されるPCRは、MPEG2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

【0133】ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体195へ格納される。

【0134】記録媒体195へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(c)に示すように間隔を詰めた状態で入力され、その後、記録媒体195に格納される。トランスポートパケットが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【0135】ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの時間カウンタが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリーカウンタである場合、24-bit長のATSが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、MPEG2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしても良い。

【0136】このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるプロ

ックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報(CCI)を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー(Copy Free)、1世代のみのコピーを許可する1世代コピー許可(One Generation Copy Allowed)、コピーを認めないコピー禁止(Copy Prohibited)などの情報が表せる。

【0137】図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン(Macrovision)のオン/オフ(On/Off)を示す情報など、様々な情報を利用することが可能である。

【0138】[キー配布構成としてのツリー(木)構造について] 次に、図1または図2に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図11は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図11の最下段に示すナンバ0~15が個々の記録再生装置である。すなわち図11に示す木(ツリー)構造の各葉(リーフ: leaf)がそれぞれの記録再生装置に相当する。

【0139】各デバイス0~15は、製造時(出荷時)に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーを自身で格納する。図11の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節(ノード)に記載されたキー: KR~K111をノードキーとする。

【0140】図11に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー: K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図11のツリーにはデバイスが0~15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが

可能である。

【0141】また、図11のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック(商標)等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図11に示すキー配布構成が適用されている。

【0142】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図11のツリー中に複数存在する。

【0143】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0144】このツリー構成において、図11から明らかのように、1つのグループに含まれる3つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスターキー: Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はK

bをKaによって暗号化したデータであることを示す。

【0145】また、ある時点tにおいて、デバイス3の所有する鍵： $K0011, K001, K00, K0, KR$ が攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー： $K001, K00, K0, KR$ をそれぞれ新たな鍵 $K(t)001, K(t)00, K(t)0, K(t)R$ に更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、 $K(t)aaa$ は、鍵 $Kaaa$ の世代（Generation）： $t$ の更新キーであることを示す。

【0146】更新キーの配布処理について説明する。キーの更新は、例えば、図12（A）に示すキー更新ブロック（KRB：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。

【0147】図12（A）に示すキー更新ブロック（KRB）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図12の例は、図11に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図11から明らかなように、デバイス0、デバイス1は、更新ノードキーとして $K(t)00, K(t)0, K(t)R$ が必要であり、デバイス2は、更新ノードキーとして $K(t)001, K(t)00, K(t)0, K(t)R$ が必要である。

【0148】図12（A）のKRBに示されるようにKRBには複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図12（A）の下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図12（A）の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図12（A）の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス0, 1は、ノードキー $K00$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00, K(t)0, K(t)R$ である。デバイス0, 1は、図12（A）の上から3段目の暗号化キー $Enc(K000, K(t)00)$ を

復号し $K(t)00$ を取得し、以下、図12（A）の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図12（A）の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス0, 1, 2は更新した鍵 $K(t)00, K(t)0, K(t)R$ を得ることができる。なお、図12（A）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0149】図11に示すツリー構造の上位段のノードキー： $K0, KR$ の更新が不要であり、ノードキー $K0$ のみの更新処理が必要である場合には、図12（B）のキー更新ブロック（KRB：Key Renewal Block）を用いることで、更新ノードキー $K(t)00$ をデバイス0, 1, 2に配布することができる。

【0150】図12（B）に示すKRBは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図11に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のマスターキー $K(t)master$ が必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たな共通の更新マスターキー： $K(t)master$ を暗号化したデータ $Enc(K(t), K(t)master)$ を図12（B）に示すKRBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0151】すなわち、デバイス0, 1, 2はKRBを処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、t時点でのマスターキー $K(t)master$ を得ることが可能になる。

【0152】[KRBを使用したマスターキーの配布] 図13に、t時点でのマスターキー $K(t)master$ を得る処理例として、 $K(t)00$ を用いて新たな共通のマスターキー $K(t)master$ を暗号化したデータ $Enc(K(t)00, K(t)master)$ と図12（B）に示すKRBとを記録媒体を介して受領したデバイス0の処理を示す。

【0153】図13に示すように、デバイス0は、記録媒体に格納されている世代：t時点のKRBと自分があるかじめ格納しているノードキー $K000$ を用いて上述したと同様のKRB処理により、ノードキー $K(t)00$ を生成する。さらに、復号した更新ノードキー $K(t)00$ を用いて更新マスターキー $K(t)master$ を復号して、後にそれを使用するために自分だけが持つリーフキー $K0000$ で暗号化して格納する。なお、デバイス0が更新マスターキー $K(t)master$ を安全に自身内に格納できる場合、リーフキー $K0000$ で暗号化する必要はない。

【0154】また、この更新マスターキーの取得処理を図14のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー:K

(c) masterを与えられ、自身のメモリに安全に(具体的にはたとえば、自身のリーフキーで暗号化して)格納しているものとする。

【0155】更新マスターキーK(n) masterとKRBの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップS1401において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーK(n) masterの時点(世代)番号:n(これを、プレ(pre-recording)記録世代情報(Generation#n)と呼ぶことにする)を読み出す。記録媒体には、予め、マスターキーK(n) masterの時点(世代)番号:nが記憶されている。また、自身が保持している暗号化マスターキーCを読み出し、ステップS1402において、その暗号化マスターキーの世代:cと、プレ記録世代情報(Generation#n)が表す世代:nとを比較して、その世代の前後を判定する。

【0156】ステップS1402において、プレ記録世代情報(Generation#n)が表す世代:nの方が、自身のメモリに記憶された暗号化マスターキーCの世代:cよりも後でない(新しくない)と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代:cが、プレ記録世代情報(Generation#n)が表す世代:nと同一か、または後の場合、ステップS1403乃至S1408をスキップして、マスターキー更新処理を終了する。即ち、この場合、自身のメモリに記憶されたマスターキーK(c) master(暗号化マスターキーC)の更新は行わないので、その更新は行われない。

【0157】一方、ステップS1402において、プレ記録世代情報(Generation#n)が表す世代:nの方が、メモリに記憶された暗号化マスターキーCの世代:cよりも後である(新しい)と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報(Generation#n)が表す世代nよりも前の世代である場合、ステップS1403に進み、記録再生装置は、記録媒体から、キー更新ブロック(KRB:Key Renewal Block)を読み出す。

【0158】ステップS1404において、記録再生装置は、ステップS1403で読み出したKRBと、自身がメモリに格納しているリーフキー(図11のデバイス0におけるK0000)およびノードキー(図11のデバイス0におけるK000、K00...)を用いて、プレ記録世代情報(Generation#n(図13におけるt)時点でのノード00の鍵K(t)00を計算する。

【0159】ステップS1405では、ステップS1404においてK(t)00を得られたか否かを確認する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク(排除)

されていることを示すので、ステップS1406乃至S1408をスキップしてマスターキー更新処理を終了する。

【0160】K(t)00を得られた場合、ステップS1406に進み、記録媒体からEnc(K(t)00, K(t) master)、すなわち、K(t)00を用いてt時点でのマスターキーを暗号化した値を読み出す。そしてステップS1407において、この暗号文をK(t)00を用いて復号してK(t) masterを計算する。

【0161】ステップS1408では、自身のみが持つリーフキー(図11のデバイス0におけるK0000)を用いてK(t) masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

【0162】ところで、マスターキーは、時点(世代)0から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数fを保持しており、その一方向性関数fに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

【0163】具体的には、例えば、記録再生装置に記憶されているマスターキーMKの世代が世代i+1であり、あるデータの再生に必要な(記録時に使用された)マスターキーMKの世代が世代i-1である場合、マスターキーK(i-1) masterは、記録再生装置において、一方向性関数fが2回用いられ、f(f(K(i+1) master))を計算することにより生成される。

【0164】また、記録再生装置に記憶されているマスターキーの世代が世代i+1であり、必要なマスターキーの世代が世代i-2である場合、マスターキーK(i-2) masterは、一方向性関数fを3回用いて、f(f(f(K(i+1) master)))を計算することにより生成される。

【0165】ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、MD5(Message Digest 5)や、SHA-1(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーK(0) master, K(1) master, K(2) master, ..., K(N) masterを、あらかじめ求めておく。即ち、まず最初に、第N世代のマスターキーK(N) masterを設定し、そのマスターキーK(N) masterに、一方向性関数を1回ずつ適用していくことで、それより前の世代のマスターキーK(N-1) master, K(N-2) master, ..., K(1) master, K(0) masterを順次生成しておく。そして、世代の小さい(前の)マスターキーK(0) masterから順番に使用してい

く。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

【0166】また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第0世代のマスターキーK(0) masterを設定し、そのマスターキーK(0) masterから使用していく。即ち、キー発行機関は、第1世代以降のマスターキーK(i) masterが必要になったら、その1世代前のマスターキーK(i-1) masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、N世代のマスターキーを、あらかじめ生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

【0167】次に、この記録再生装置がコンテンツを自身の記録媒体に記録する場合の、記録再生装置の処理について図15のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

【0168】まず最初に、ステップS1501において、記録再生装置は、記録媒体から、プレ記録世代情報Generation#nを読み出す。また、自身のメモリが記憶している暗号化マスターキーCの世代cを取得し、ステップS1502において、その暗号化マスターキーの世代cと、プレ記録世代情報Generation#nが表す世代nとを比較して、その世代の前後を判定する。

【0169】ステップS1502において、メモリに記憶された暗号化マスターキーCの世代cが、プレ記録世代情報Generation#nが表す世代n以後でないと判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代cが、プレ記録世代情報Generation#nが表す世代nよりも古い世代である場合、ステップS1503をスキップして、すなわち、コンテンツデータの記録処理を行わずに終了する。

【0170】一方、ステップS1502において、自身の記録再生装置内のメモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代n以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代nと同一か、またはそれよりも新しい場合、ステップS1503に進み、コンテンツデータの記録処理を行う。

【0171】〔世代管理のなされたマスターキーによるコンテンツデータ暗号化および記録処理〕以下、世代管理のなされたマスターキーによってコンテンツデータの暗号化処理を実行して、自己の記録媒体に格納する処理について説明する。なお、ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用したデータに基づいてブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。また、記録再生装置が記録媒体に記録したデータを他の再生機器において再生可能とする設定と再生不可能とする設定が可能な構成を例として説明する。

【0172】図16、図17の処理ブロック図および図18のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクID(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

【0173】図16、図17の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理の概要について説明する。

【0174】記録再生装置1600は自身のメモリ180(図1、2参照)に格納しているマスターキー1601、デバイス識別子としてのデバイスID1631、デバイス固有キー1632を読み出す。マスターキー1601は、ライセンスを受けた記録再生装置に格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図11に示す点線枠のグループに属するデバイスに共通なキーである。デバイスIDは記録再生装置1600の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスIDは公開されていてもよい。デバイス固有キーは、その記録再生装置1600に固有の秘密鍵であり、予め個々の記録再生装置に応じて異なるように設定されて格納されたキーである。これらは予め記録再生装置1600のメモリに格納されている。

【0175】記録再生装置1600は例えば光ディスクである記録媒体1620に識別情報としてのディスクID(Disc ID)1603が既に記録されているかどうかを検査する。記録されていれば、ディスクID(Disc ID)1603を読み出し(図16に相当)、記録されていなければ、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID(Disc ID)1701を生成し、ディスクに記録する(図17に相当)。ディスクID(Disc ID)1603はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0176】記録再生器1600は、次にマスターキーとディスクIDを用いて、ディスク固有キー(Disc Unique Key)を生成1602する。ディスク固有キー(Disc Unique Key)の具体的な生成方法としては、図19に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー(Master Key)とディスクID(Disc ID)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID(Disc ID)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する例2の方法が適用できる。

【0177】次に、記録ごとの固有鍵であるタイトルキー(Title Key)を暗号処理手段150(図1, 2, 参照)においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成1604し、ディスク1620に記録する。

【0178】さらに、このタイトル(データ)がデータ記録を実行した記録再生装置でのみ再生可能とする(機器制限あり)か、他の機器においても再生可能とする(再生機器制限なし)のいずれであるかを示すフラグ、すなわち再生機器制限フラグ(Player Restriction Flag)を設定し1633、ディスク1620に記録する1635。さらに、機器識別情報としてのデバイスID取り出して1631、ディスク1620に記録する1634。

【0179】さらに、使用するマスターキーの世代番号、すなわち、自身が格納するマスターキーの世代番号[記録時世代番号(Generation#)]1650を取得して、これを記録媒体1620に記録時世代番号1651として格納する。

【0180】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー1605、再生機器制限フラグ1635、デバイスID1634、マスターキーの世代番号[記録時世代番号(Generation#)]1651を格納することができる。

【0181】なお、記録媒体1620には、予め、プレ(pre-recording)世代番号が格納されており、プレ世代番号と同一またはプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

【0182】次にディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスID、あるいは、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キー、いずれかの組合せから、タイトル固有キー(Title Unique Key)を生成する。

【0183】すなわち、再生機器制限をしない場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスIDとからタイトル固有キー(Title Unique Key)を生成し、再生機器制限をする場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キーとからタイトル固有キー(Title Unique Key)を生成する。

【0184】このタイトル固有キー(Title Unique Key)生成の具体的な方法は、図21に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー(Title Key)とディスク固有キー(Disc Unique Key)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID(Disc ID)とデバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー(Title Unique Key)として使用する例2の方法が適用できる。

【0185】なお、上記の説明では、マスターキー(Master Key)とディスクID(Disc ID)からディスク固有キー(Disc Unique Key)を生成し、これとタイトルキー(Title Key)とデバイスID、もしくはタイトルキー(Title Key)とデバイス固有キーからタイトル固有キー(Title Unique Key)をそれぞれ生成するようにしているが、ディスク固有キー(Disc Unique Key)を不要としてマスターキー(Master Key)とディスクID(Disc ID)とタイトルキー(Title Key)と、デバイスIDもしくはデバイス固有キーから直接タイトル固有キー(Title Unique Key)を生成してもよく、また、タイトルキー(Title Key)を用いずに、マスターキー(Master Key)とディスクID(Disc ID)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)からタイトル固有キー(Title Unique Key)相当の鍵を生成してもよい。

【0186】ところで、たとえば上記のSCDTCに規定される伝送フォーマットのひとつを使用した場合、データはMPEG2のTSパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス(STB: Set Top Box)がこの放送を記録機にSCDTCを用いて伝送する際に、STBは衛星放送通信路で伝送されたMPEG2 TSパケットをIEEE 1394上も伝送することが、データ変換の必要がなく望ましい。

【0187】記録再生装置1600は記録すべきコンテンツデータをこのTSパケットの形で受信し、前述したTS処理手段300において、各TSパケットを受信した時刻情報であるATSを付加する。なお、先に説明し



たように、ブロックデータに付加されるブロック・シードは、ATSとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

【0188】ATSを付加したTSパケットをX個（例えばX=32）並べて、1ブロックのブロックデータが形成（図5の上の図参照）され、図16、17の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1～4バイトが分離され（セクタ1608）で出力される32ビットのATSを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成1607される。

【0189】ブロック・キー（Block Key）の生成方法の例を図22に示す。図22では、いずれも32ビットのブロック・シード（Block Seed）と、64ビットのタイトル固有キー（Title Unique Key）とから、64ビットのブロックキー（Block Key）を生成する例を2つ示している。

【0190】上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と32ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

【0191】例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をSHA-1に入力し、その160ビットの出力を、たとえば下位64ビットのみ使用するなど、64ビットに縮約したものをブロックキー（Block Key）としている。

【0192】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごと MASTER キー（Master Key）とディスクID（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイスID（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（Block Key）を生成してもよい。

【0193】ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図16、17の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第1～mバイト（たとえばm=8バイト）は分離（セクタ1608）されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化1609する。なお、暗号化されないmバイト中にはブロック・シードとしての

第1～4バイトも含まれる。セクタ1608により分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化1609される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるDES（Data Encryption Standard）を用いることができる。

【0194】ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がDESのように8バイトであるときは、Xを例えば32とし、mを例えば8の倍数とすることで、端数なくm+1バイト目以降のブロックデータ全体が暗号化できる。

【0195】すなわち、1ブロックに格納するTSパケットの個数をX個とし、暗号アルゴリズムの入出力データサイズをLバイトとし、nを任意の自然数とした場合、 $192 * X = m + n * L$  が成り立つようにX、m、Lを定めることにより、端数処理が不要となる。

【0196】暗号化した第m+1バイト以降のブロックデータは暗号処理のされていない第1～mバイトデータとともにセクタ1610により結合されて暗号化コンテンツ1612として記録媒体1620に格納される。

【0197】以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ATSを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。

【0198】上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、すなわち再生可能となる条件となる。

【0199】さらに、ブロックキーは上述のように再生機器制限をしない場合は、デバイスIDに基づいて生成され、再生機器制限をする場合は、デバイス固有キーに基づいて生成される。これらの暗号化データは、再生機器制限をした場合は、そのデータを記録した機器でのみ再生可能となる。

【0200】すなわち、再生機器制限なしの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイスIDを含むデータに基づいて生成されるとともに、デバイスIDが記録媒体に格納される。従って、記録媒体上のコンテンツを再生しようとする機器は、記録媒体からデバイスIDを取得可能であり、同様のブロックキーを生成することが可能となるのでブロックデータの復号が可能となる。しかし、再生機器制限ありの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイス固有キーを含むデータに基づいて生成される。このデバイス固有キーはデバイス毎に異なる秘密鍵であり、他の機器は、そのキーを取得することはできない。また、ブロックデータを暗号化して記録媒体に格納する場合、

デバイス固有キーの記録媒体に対する書き込み処理は実行されない。従って、他の再生機器では、暗号化されたブロックデータを格納した記録媒体を装着しても、同一のデバイス固有キーを取得することができないので、ブロックデータを復号するための復号キーを生成することができず、復号不可能となり再生できない。なお、再生処理の詳細については後述する。

【0201】次に図18に示すフローチャートに従って、データ記録処理にともなって実行されるTS処理手段300におけるATS付加処理および暗号処理手段150における暗号処理の処理の流れを説明する。図18のS1801において、記録再生装置は自身のメモリ180に格納しているマスターキー、デバイス識別子としてのデバイスID、デバイス固有キーを読み出す。

【0202】S1802において、記録媒体に識別情報としてのディスクID(Disc ID)が既に記録されているかどうかを検査する。記録されていればS1803でこのディスクIDを読み出し、記録されていなければS1804で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S1805では、マスターキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することである。

【0203】次にS1806に進み、その一回の記録ごとの固有の鍵としてのタイトルキー(Title Key)、再生機器制限フラグ(Player Restriction Flag)、さらに、機器識別情報としてのデバイスID、マスターキーの世代番号を取り出してディスクに記録する。次にS1807で、上記のディスク固有キーとタイトルキーと、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)から、タイトル固有キーを生成する。

【0204】タイトル固有キーの生成の詳細フローを図20に示す。暗号処理手段150は、ステップS2001において、再生機器制限をするかしないかの判定を実行する。この判定は、記録再生器を使用するユーザによって入力された指示データ、あるいはコンテンツに付加された利用制限情報に基づいて判定する。

【0205】S2001の判定がNo、すなわち、再生機器制限をしない場合は、ステップS2002に進み、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスIDとから、タイトル固有キー(Title Unique Key)を生成する。

【0206】S2001の判定がYes、すなわち、再生機器制限をする場合は、ステップS2003に進みディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キーとから、タイトル固有

キー(Title Unique Key)を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0207】S1808では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1809で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1810で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1811に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0208】次に、暗号処理手段150は、S1812で、ブロックデータの先頭の32ビット(ATSを含むブロック・シード)とS1807で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0209】S1813では、ブロックキーを用いてS1811で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES(Data Encryption Standard)が適用される。

【0210】S1814で、暗号化したブロックデータを記録媒体に記録する。S1815で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS1808に戻って残りのデータの処理を実行する。

【0211】[世代管理のなされたマスターキーによるコンテンツデータ復号および再生処理]次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図23の処理ブロック図と、図24～図26のフローチャートを用いて説明する。

【0212】図23の処理ブロック図を参照しながら、図24に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図24のS2401において、記録再生装置2300はディスク2320からディスクID2302とプレ(pre-recording)記録世代番号を読み出し、また自身のメモリからマスターキー2301、デバイス識別子としてのデバイスID2331、デバイス固有キー2332を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクにあらかじめ記録されているか、そうでない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。

【0213】プレ (pre-recording) 記録世代番号2360は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このプレ (pre-recording) 世代番号と、データ記録時のマスターキーの世代番号、すなわち記録時世代番号2350を比較して再生処理の可否を制御する。マスターキー2301は、ライセンスを受けた記録再生装置に格納され世代管理のなされた秘密キーであり、デバイスIDは記録再生装置固有の識別子、デバイス固有キーは、その記録再生器に固有の秘密鍵である。

【0214】記録再生装置2300は、次に、S2402で、ディスクから読み出すべきデータのタイトルキー、さらに、このデータを記録した記録再生器のデバイスIDと、データに対応して設定された再生機器制限フラグ、データを記録したときに使用したマスターキーの世代番号 (Generation #) すなわち記録時世代番号2350を読み出す。次に、S2403で読み出すべきデータが再生可能か否かを判定する。判定の詳細フローを図25に示す。

【0215】図25のステップS2501において、記録再生装置は、S2401で読み出したプレ世代番号と、S2402で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、プレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、プレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

【0216】即ち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

【0217】一方、ステップS2501において、記録時世代番号が表す世代が、プレ記録世代番号が表す世代以後であると判定された場合、即ち、記録時世代情報が表す世代が、プレ記録世代番号が表す世代nと同一か、または新しい世代であり、従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステップS2502に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーCの世代情報を取得し、その暗号化マスターキーの世代と、暗

号時世代情報が表す世代を比較して、その世代の前後を判定する。

【0218】ステップS2502において、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。

【0219】一方、ステップS2502において、メモリに記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代と同一か、またはそれよりも新しい場合、ステップS2503に進み、読み出しをしたいデータが再生機器制限されて記録されているかどうかを検査する。

【0220】ステップS2503では、読み出した再生機器制限フラグの示す再生機器制限情報が、「再生機器制限あり」の設定であるか否かを判定する。ありの場合は、ステップS2504において、「記録媒体から読み出したデバイスIDと自己のデバイスIDが一致するか否か」を判定する。一致する場合は、再生可能と判定する。ステップS2503において、「再生機器制限あり」の設定でないと判定された場合も、再生可能と判定する。読み出した再生機器制限フラグが示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスIDと自己のデバイスIDが一致しない」場合は、再生不可能と判定する。

【0221】再生可能と判定された場合は、ステップS2404に進む。S2404では、ディスクID (Disc ID) とマスターキー (Master Key) を用いてディスク固有キー (Disc Unique Key) を生成2303する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する手法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、S2402で記録媒体から読み出した、そのデータの記録時世代番号が表す世代 (時点) のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、前述した方法を用いて記録時世代番号が表す世代のマスターキーを作成し、それを用いてディスク固有キー (Disc Unique Key) を生成してもよい。

【0222】次に、S2405で、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを

図26に示す。暗号処理手段150は、ステップS2601において、再生機器制限をするの設定であるか、しないの設定であるかの判定を実行する。この判定は、ディスクから読み出した再生機器制限フラグに基づいて実行される。

【0223】データを記録した記録再生器のデバイスID2334と、データに対応して設定された再生機器制限フラグ2335を読み出し、読み出した再生機器制限フラグ2335が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスID2334と自己のデバイスID2331が一致する」か、あるいは、読み出した再生機器制限フラグ2335が示す再生機器制限情報が、「再生機器制限なし」である場合は、再生可能となり、読み出した再生機器制限フラグ2335が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスID2334と自己のデバイスID2331が一致しない」場合は、再生不可能となる。

【0224】再生不可能とされる場合は、データは、そのデータを記録した記録再生器固有のデバイス固有キーに基づいて生成されたブロックキーによって暗号化されており、そのデータを記録した記録再生器以外の記録再生器は同一のデバイス固有キーを保有しないので、データを復号するためのブロックキーを生成することができない場合である。

【0225】再生可能である場合は、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスID、あるいは、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キー、いずれかの組合せから、タイトル固有キー(Title Unique Key)を生成する。

【0226】すなわち、再生機器制限をしない設定である場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスIDとからタイトル固有キー(Title Unique Key)を生成し、再生機器制限をする設定である場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、自己のデバイス固有キーとからタイトル固有キー(Title Unique Key)を生成する。このキー生成方法としては、ハッシュ関数SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

【0227】図26のフローに従って説明する。S2601の判定がNo、すなわち、再生機器制限をしない設定である場合は、ステップS2602に進み、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスIDとから、タイトル固有キー(Title Unique Key)を生成する。

【0228】S2601の判定がYes、すなわち、再生機器制限をする場合は、ステップS2603に進みディスク固有キー(Disc Unique Key)とタイトルキー(T

itleKey)と、自己の記録再生器の有するデバイス固有キーとから、タイトル固有キー(Title Unique Key)を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0229】なお、上記の説明では、マスターキー(Master Key)とディスクID(Disc ID)からディスク固有キー(Disc Unique Key)を生成し、これとタイトルキー(Title Key)とデバイスID、もしくはタイトルキー(Title Key)とデバイス固有キーからタイトル固有キー(Title Unique Key)をそれぞれ生成するようにしているが、ディスク固有キー(Disc Unique Key)を不要としてマスターキー(Master Key)とディスクID(Disc ID)とタイトルキー(Title Key)と、デバイスIDもしくはデバイス固有キーから直接タイトル固有キー(Title Unique Key)を生成してもよく、また、タイトルキー(Title Key)を用いずに、マスターキー(Master Key)とディスクID(Disc ID)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)からタイトル固有キー(Title Unique Key)相当の鍵を生成してもよい。

【0230】次にS2406でディスクから暗号化されて格納されている暗号化コンテンツ2312から順次ブロックデータ(Block Data)を読み出し、S2407で、ブロックデータの先頭の4バイトのブロック・シード(Block Seed)をセクタ2310において分離して、ブロックシード(Block Seed)と、S2405で生成したタイトル固有キーを用いてブロックキーを生成する。

【0231】ブロック・キー(Block Key)の生成方法は、先に説明した図22の構成を適用することができる。すなわち、32ビットのブロック・シード(Block Seed)と、64ビットのタイトル固有キー(Title Unique Key)とから、64ビットのブロックキー(Block Key)を生成する構成が適用できる。

【0232】なお、上記ではディスク固有キー(Disc Unique Key)、タイトル固有キー(Title Unique Key)、ブロックキー(Block Key)をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー(Disc Unique Key)とタイトル固有キー(Title Unique Key)の生成を実行することなく、ブロックごとにマスターキー(Master Key)とディスクID(Disc ID)とタイトルキー(Title Key)と、ブロックシード(Block Seed)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)を用いてブロックキー(Block Key)を生成してもよい。

【0233】ブロックキーが生成されると、次にS2408で、ブロックキー(Block Key)を用いて暗号化されているブロックデータを復号2309し、セクタ2308を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各ト

ランスポートバケットにATSが付加されており、先に説明したTS処理手段300において、ATSに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

【0234】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。ブロック鍵を用いて暗号化されているブロックデータを復号し、S2409で、全データを読み出したかを判断し、全データを読み出してれば終了し、そうでなければS2406に戻り残りのデータを読み出す。

【0235】〔記録媒体にのみ有効なメディアキーを使用した処理構成〕ところで、上記の実施例においては、キー更新ブロックKRB: Key Renewal Blockを用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うとしている。

【0236】マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点およびそれ以前にこのシステムで記録されたデータを復号することが可能になる。ただし、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

【0237】これに対し、記録媒体のKRB (Key Renewal Block) を用いて伝送する鍵として、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることも可能である。以下に、第2の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。ただし、第1の実施例との変更部分のみを説明する。

【0238】図27には、図13と同様の例として、デバイス0が記録媒体に格納されているt時点のKRBと自分があらかじめ格納しているリーフキーK0000とノードキーK000、K00を用いて更新ノードキーK(t)00を生成し、それを用いて更新メディアキー: K(t) mediaを得る様子を示している。ここで得たK(t) mediaは、その記録媒体のデータの記録、再生時に使用される。

【0239】なお、図27におけるブレ記録世代番号(Generation #n)は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオプションとして設定される。

【0240】各記録再生装置は、たとえば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図28に示すフローチャートによってその記録媒体用のメディアキー: K(t) mediaを計算し、後にその記録媒体へのアクセスに使用する。

【0241】図28のステップS2801のKRBの読みこみとS2802のKRBの処理は、それぞれ図14のステップS1403およびS1404と同様の処理である。

【0242】ステップS2803において記録再生装置はメディアキーK(t) mediaをノードキー K(t) 00で暗号化した暗号文Enc(K(t)00, K(t) media)を記録媒体から読みこみ、ステップS2804でこれを復号してメディアキーを得る。もしこの記録再生装置が図11に示すツリー構成のグループから排除、すなわちリボークされていれば、メディアキーを入手できず、その記録媒体への記録および再生が行えない。

【0243】次に、記録媒体へのデータの記録の処理を説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第1の実施例において図15に示した、ブレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図29に示す処理フローようになる。図29の処理フローは、メディアキーの取得をS2901で判定し、取得された場合にのみ、ステップS2902においてコンテンツの記録処理を実行するものである。

【0244】〔記録媒体にのみ有効なメディアキーを使用したデータの記録処理〕コンテンツデータの記録処理の様子を、図30、31のブロック図および図32のフローチャートを用いて説明する。

【0245】本実施例では、第1の実施例と同様、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクID(Disc ID)を、データを暗号化する鍵に作用させるようにしている点も同様である。

【0246】図30および図31は、それぞれ第1の実施例における図16および図17に対応する図であり、マスターキー(Master Key)の代わりにメディアキー(Media Key)が使われている点が異なっており、また、マスターキーの世代を示す記録時代番号(Generation #)を用いていない点が異なっている。図30および図31の差異は、図16、図17の差異と同様ディスクIDの書き込みを実行するかしないかの差異である。

【0247】図32はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、実施例1の図18のフローチャートに対応する。以下、図32の処理フローについて実施例1と異なる点を中心として説明する。

【0248】図32のS3201において、記録再生装置3000は自身のメモリに格納している機器識別情報(Device ID)、機器固有鍵(Device Unique Key)と、図28のS2804で計算し、一時的に保存しているメ

メディアキーK (t) mediaを読み出す。

【0249】S3202において、記録再生装置は記録媒体（光ディスク）3020に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていれば、S3203でこのディスクID (Disc ID) を読み出し（図30に相当）、記録されていないければ、S3204で、ランダムに、もしくはあらかじめ定められた方法でディスクID (Disc ID) を生成し、ディスクに記録する（図31に相当）。ディスクID (Disc ID) はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次にS3205に進む。

【0250】S3205では、S3201で読み出したメディアキーとディスクID (Disc ID) を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、第1の実施例で使用した方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

【0251】次にS3206に進み、その一回の記録ごとに固有の鍵：タイトルキー (Title Key) をランダムに、あるいはあらかじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル（データ）が、記録した機器でのみ再生できるもの（再生機器制限する）か、他の機器でも再生できる（再生機器制限しない）かを表す情報としての再生機器制限フラグ (Player Restriction Flag) と、記録機器が持つ機器識別情報 (Device ID) をディスクに記録する。

【0252】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、再生機器制限フラグ (Player Restriction Flag)、機器識別情報 (Device ID) を格納することができる。

【0253】ステップS3207乃至S3215は図18のS1807乃至S1815と同様であるため説明を省略する。

【0254】なお、上記の説明では、メディアキー (Media Key) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデバイスID、もしくはタイトルキー (Title Key) とデバイス固有キーからタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とディスクID (Disc ID) とタイトルキー (Title Key) と、デバイスIDもしくはデバイス固有キーから直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) とディスクID (Disc ID) と、デバイスID（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー

(Title Unique Key) 相当の鍵を生成してもよい。

【0255】以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

【0256】〔記録媒体にのみ有効なメディアキーを使用したデータの再生処理〕次に、上記のようにして記録されたデータを再生する処理の様子を図33のブロック図と図34のフローチャートを用いて説明する。

【0257】図33は、第1の実施例における図23に対応する図であり、マスターキー (Master Key) の代わりにメディアキー (Media Key) が使われ、そのため記録時世代番号 (Generation #) が省略されている点が異なっている。

【0258】図34のS3401において、記録再生装置3400は記録媒体であるディスク3420からディスクID (Disc ID) を、また自身のメモリから自己の機器識別情報としてデバイスID (Device ID)、自己の機器固有鍵であるデバイス固有キー (Device Unique Key) と、図28のS2804で計算し一時的に保存しているメディアキーを読み出す。

【0259】なお、この記録媒体の挿入時に、図28の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

【0260】次にS3402で、ディスクから読み出すべきデータのタイトルキー (Title Key) とこのデータを記録した機器のデバイスID (Device ID) とこのデータの再生機器制限フラグ (Player Restriction Flag) を読み出す。

【0261】次にS3403で、このデータが再生可能であるかを判断する。S3403の処理の詳細を図35に示す。

【0262】ステップS3501ではメディアキー (Media Key) を得られたか否かを判定する。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップS3502に進む。ステップS3502およびS3503の処理は図25のS2503およびS2504とそれぞれ同じであり、再生機器制限フラグ (Player Restriction Flag) が表す再生機器制限の状態が、「再生機器制限されている」であり、かつ、S3503で記録媒体から読み出した記録した機器のデバイスID (Device ID) と、S3401でメモリから読み出した自己のデバイスID (Device ID) により、「記録した機器が自分ではない」という2つの条件が重なった場合には「再生不可能」と判断し、ステップS3404乃至S3409をスキップして、再生処理を行わずに処理を終了し、一方それ以外の場合には「再生可能」と判断してS3404に進む。

【0263】ステップS3404乃至S3409の処理は、図24のS2404乃至S2409と同様であるため、説明を省略する。

【0264】なお、上記の説明では、メディアキー (Media Key)

dia Key) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデバイスID、もしくはタイトルキー (Title Key) とデバイス固有キーからタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とディスクID (Disc ID) とタイトルキー (Title Key) と、デバイスIDもしくはデバイス固有キーから直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) とディスクID (Disc ID) と、デバイスID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0265】上記のようにして、記録媒体へのデータの記録および記録媒体からの再生が行える。

【0266】「記録再生装置による記録媒体へのキー更新ブロック (KRB) 格納処理」ところで、上述した例では、キー更新ブロック: KRB (Key Renewal Block) が記録媒体にあらかじめ格納されている例を示したが、図36に示すように、記録再生装置3600が入出力I/F120、140や、モデム3601等を介して他の機器から受信したKRB (Key Renewal Block) を、最初に記録媒体にデータを記録する際や、記録媒体にデータを記録するたびに記録媒体に記録するようにすることもできる。

【0267】すなわち、たとえば第1の実施例において、図37に示すように、記録再生装置はあらかじめ、入出力I/F120、140やモデム3601等を介してキー更新ブロック: KRB (Key Renewal Block) とマスターキーをノードキーで暗号化した暗号文を入手し、自身の記憶手段であるメモリ180等に格納しておき、コンテンツデータの記録媒体に対する記録の際に、図38に示すフローチャートに従って処理をする構成としてもよい。

【0268】図38の処理フローについて説明する。ステップS3801において、データを記録しようとする記録媒体にはすでにキー更新ブロック: KRB (Key Renewal Block) が記録されているか否かを検査する。すでに記録媒体にキー更新ブロック: KRB (Key Renewal Block) が記録されていた場合にはステップS3802をスキップして終了する (データの記録処理に進む) が、記録されていない場合には、ステップS3902に進み、図39に示すように、自身の記憶手段、例えばメモリ180に格納しているキー更新ブロック: KRB (Key Renewal Block) とマスターキーを暗号化した暗号文を記録媒体に記録する処理を実行する。その処理の実行の後に、コンテンツデータの記録処理に進む。

【0269】この方法は、マスターキーに特化したもの

ではなく、たとえば第2の実施例のようにメディアキーを用いる記録方法に適用することももちろん可能である。

【0270】「記録処理におけるコピー制御」さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0271】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの (コピー可能) かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0272】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1または図2の記録再生装置の処理について、図40および図41のフローチャートを参照して説明する。

【0273】まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図40

(A) のフローチャートにしたがった記録処理が行われる。図40 (A) の処理について説明する。図1の記録再生器100を例として説明する。デジタル信号のコンテンツ (デジタルコンテンツ) が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS4001において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS4002に進む。

【0274】ステップS4002では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合 (例えば、上述のDTC Pを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合) には、そのコンテンツは、コピー可能であると判定される。

【0275】また、記録再生装置100がDTC Pに準拠している装置であるとし、DTC Pに従って処理を実行するものとする。DTC Pでは、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator) が規定されている。EMIが00B (Bは、その前の値が2進数であることを表す) である場合は、コンテンツがコピーフリーのもの (Copy-free) であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの (No-more-copies) であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの (Copy-one-generation) であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの (Copy-never) であるこ

とを表す。

【0276】記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【0277】ステップS4002において、コンテンツがコピー可能でないと判定された場合、ステップS4003～S4005をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0278】また、ステップS4002において、コンテンツがコピー可能であると判定された場合、ステップS4003に進み、以下、ステップS4003～S4005において、図3(A)のステップS302、S303、S304における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0279】なお、EMIは、入出力I/F120に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報（例えば、DTCFにおけるembedded CCIなど）も記録される。

【0280】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【0281】本発明の記録再生装置では、このEMIやembedded CCIなどのコピー制御情報を、TSパケットに付加する形で記録する。即ち、図10の例2や例3のように、ATSを24ビットないし30ビット分と、コピー制御情報を加えた32ビットを図5に示すように各TSパケットに付加する。

【0282】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図40(B)のフローチャートにしたがった記録処理が行われる。図40(B)の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力I/F140に供給されると、入出力I/F140は、ステップS4011において、そのアナログコンテンツを受信し、ステップS4012に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0283】ここで、ステップS4012の判定処理は、例えば、入出力I/F140で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれ

るかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F140で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0284】また、例えば、CGMS-A信号は、デジタル信号のコピー制御に用いられるCGMS信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであることを表す。

【0285】従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【0286】さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【0287】ステップS4012において、アナログコンテンツがコピー可能でないと判定された場合、ステップS4013乃至S4017をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0288】また、ステップS4012において、アナログコンテンツがコピー可能であると判定された場合、ステップS4013に進み、以下、ステップS4013乃至S4017において、図3(B)のステップS322乃至S326における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MPEG符号化、TS処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【0289】なお、入出力I/F140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。即ち、図10で示したCCIもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0290】〔再生処理におけるコピー制御〕次に、記録媒体に記録されたコンテンツを再生して、デジタル



コンテンツとして外部に出力する場合においては、図41(A)のフローチャートにしたがった再生処理が行われる。図41(A)の処理について説明する。まず最初に、ステップS4101、S4102、S4103において、図41(A)のステップS401、S402、S403における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段150において復号処理がなされ、TS処理がなされる。各処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F120に供給される。

【0291】入出力I/F120は、ステップS4104において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI、あるいは、EMIと同様にコピー制御状態を表す情報(コピー制御情報)が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0292】また、例えば、入出力I/F120に供給されるデジタルコンテンツにEMIが含まれる場合、従って、コンテンツの記録時に、DTC Pの規格にしたがって、EMIが記録された場合には、そのEMI(記録されたEMI(Recorded EMI))が、Copy-freelyであるときには、デジタルコンテンツは、後でコピー可能なものであると判定される。また、EMIが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【0293】なお、一般的には、記録されたEMIが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのEMIは記録時にNo-more-copiesに変換され、また、Copy-neverのEMIを持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0294】ステップS4104において、コンテンツが、後でコピー可能なものであると判定された場合、ステップS4105に進み、入出力I/F120は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0295】また、ステップS4104において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップS4106に進み、入出力I/F120は、例えば、DTC Pの規格等にしたがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0296】即ち、例えば、上述のように、記録されたEMIが、No-more-copiesである場合(もしくは、シス

テムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIがCopy-one-generationである場合には、コンテンツは、それ以上のコピーは許されない。

【0297】このため、入出力I/F120は、DTC Pの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合(ここでは、DTC Pの規格に準拠した装置である場合)には、デジタルコンテンツを暗号化して、外部に出力する。

【0298】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図41(B)のフローチャートにしたがった再生処理が行われる。図41(B)の処理について説明する。ステップS4111乃至S4115において、図41(B)のステップS421乃至S425における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、TS処理、MPEGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

【0299】入出力I/F140は、ステップS4116において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにEMIなどのコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0300】また、コンテンツの記録時に、例えばDTC Pの規格にしたがって、EMIまたはコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0301】また、EMIまたはコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIまたはコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【0302】さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【0303】ステップS4116において、コンテンツが、後でコピー可能であると判定された場合、ステップS4117に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0304】また、ステップS4116において、コンテンツが、後でコピー可能でないと判定された場合、ステップS4118に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0305】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0306】このため、入出力I/F140は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すGCMS-A信号を付加して、外部に出力する。また、例えば、記録されたGCMS-A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I/F140は、GCMS-A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【0307】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【0308】〔データ処理手段の構成〕なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段150は暗号化/復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にTS処理手段300も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図42は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0309】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク4205やROM4203に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-

ROM(Compact Disc Read Only Memory)、MO(Magnetooptical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体4210に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体4210は、いわゆるパッケージソフトウェアとして提供することができる。

【0310】なお、プログラムは、上述したようなリムーバブル記録媒体4210からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local AreaNetwork)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部4208で受信し、内蔵するハードディスク4205にインストールすることができる。

【0311】コンピュータは、CPU(Central Processing Unit)4202を内蔵している。CPU4202には、バス4201を介して、入出力インタフェース4211が接続されており、CPU4202は、入出力インタフェース4210を介して、ユーザによって、キーボードやマウス等で構成される入力部4207が操作されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)4203に格納されているプログラムを実行する。

【0312】あるいは、CPU4202は、ハードディスク4205に格納されているプログラム、衛星若しくはネットワークから転送され、通信部4208で受信されてハードディスク4205にインストールされたプログラム、またはドライブ4209に装着されたリムーバブル記録媒体4210から読み出されてハードディスク4205にインストールされたプログラムを、RAM(Random Access Memory)4204にロードして実行する。

【0313】これにより、CPU4202は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU4202は、その処理結果を、必要に応じて、例えば、入出力インタフェース4211を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部4206から出力、あるいは、通信部4208から送信、さらには、ハードディスク4205に記録させる。

【0314】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0315】また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュ

ータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0316】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1および図2に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU170が実行する1つのソフトウェアモジュールとして実現することが可能である。

【0317】〔記録媒体の製造装置および方法〕次に、上述した本発明の情報記録媒体を製造する本発明の情報記録媒体製造装置および方法について説明する。

【0318】図43には、記録媒体を製造すると共に、記録媒体に対してディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録するディスク製造装置の概略構成を示す。

【0319】この図43に示すディスク製造装置は、図示しない組立工程により既に組み立てられている情報記録媒体に対して、ディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録する。さらに、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) も併せて記録する。

【0320】ディスク製造装置4300は、ディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーをあらかじめ格納しているメモリ4302もしくはその他の記憶手段と、記録媒体4350に対する読み書きを行う記録媒体I/F4303と、他の装置とのI/Fとなる入出力I/F4304と、それらを制御する制御部4301、これらを接続するバス4305を備えている。

【0321】なお、図43の構成では、メモリ4302および記録媒体I/F4304は、当該製造装置に内蔵されている例を挙げているが、メモリ4302および記録媒体I/F4303は外付けのものであってもよい。

【0322】上記のディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) は、たとえば図示しない鍵発行センタにより発行されるものであり、上記内蔵あるいは外付けのメモリにあらかじめ格納されている。

【0323】上記メモリ4302に格納されているディスクID (Disk ID)、キー更新ブロック：KRB (Key

Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーは、制御部4301の制御の下、記録媒体I/F4303を介して記録媒体に記録される。なお、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) についても記録する。

【0324】また、ディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) は、上述したようにメモリ4302にあらかじめ格納されているものを使用するだけでなく、たとえば入出力I/F4304を介して鍵発行センタから送られてきたものを入手することも可能である。

【0325】図44には、本発明の記録媒体製造方法として、上記記録媒体を製造すると共に、記録媒体に対してディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) を記録する記録媒体製造方法における製造工程の流れを示す。

【0326】図44において、記録媒体製造方法では、まず、ステップS4401の製造工程として、図示しない公知の組立工程によりDVD、CD等各種記録媒体が組み立てられる。

【0327】次に、ステップS4402の製造工程として、図43の記録媒体製造装置により、製造された記録媒体に対して、ディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーの記録処理を実行する。また、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) を記録する。

【0328】以上のディスク製造処理プロセスにより、記録媒体は、ディスクID (Disk ID)、キー更新ブロック：KRB (Key Renewal Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録した状態で製造工場から出荷される。また、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) を記録した後、製造工場から出荷される。

【0329】〔KRBのフォーマット〕図45にキー更新ブロック (KRB: Key Renewal Block) のフォーマット例を示す。バージョン4501は、キー更新ブロック (KRB: Key Renewal Block) のバージョンを示す識別子である。デプス4502は、キー更新ブロック (KRB: Key Renewal Block) の配布先のデバイスに対する階層ツリーの階層数を示す。データポイント4503は、キー更新ブロック (KRB: Key Renewal Block)

k) 中のデータ部の位置を示すポイントであり、タグポイント4504はタグ部の位置、署名ポイント4505は署名の位置を示すポイントである。データ部4506は、例えば更新するノードキーを暗号化したデータを格納する。

【0330】タグ部4507は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図46を用いて説明する。図46では、データとして先に図12(A)で説明したキー更新ブロック(KRB)を送付する例を示している。この時のデータは、図46の右の表に示ようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーK(t)Rが含まれているので、トップノードアドレスはKRとなる。

【0331】暗号化キーの最上段のデータEnc(K(t)0, K(t)R)は、図46の左の階層ツリーに示す位置にある。ここで、次のデータは、Enc(K(t)00, K(t)0)であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは{左(L)タグ, 右(R)タグ}として設定される。最上段のデータEnc(K(t)0, K(t)R)の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図46(c)に示すデータ列、およびタグ列が構成される。ツリーのノードの処理の順序として同一段の幅方向を先に処理するwidth firstと、深さ方向を先に処理するdepth firstのいずれかを用いるのが好適である。

【0332】図45に戻って、KRBフォーマットについてさらに説明する。署名(Signature)は、キー更新ブロック(KRB)を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。KRBを受領したデバイスは署名検証によって正当なキー更新ブロック(KRB)を発行者が発行したキー更新ブロック(KRB)であることを確認する。

【0333】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0334】

【発明の効果】以上、説明したように、本発明の情報記録再生装置によれば、ツリー(木)構造の鍵配布構成により、マスターキーやメディアキーの更新データを更新ブロック(KRB)とともに送信する構成としたので、鍵更新の必要なデバイスにのみ復号可能な構成とした伝

送または配布が可能となり、メッセージ量を小さく抑えることができる。さらに、ツリー構造によって規定される特定のグループにのみ復号可能な鍵をメッセージ量を少なくして配布可能であり、グループに属さない他のデバイスには復号できない構成とすることが可能であり、キー配信または配布の安全性が確保される。

【0335】また、ツリー構造の鍵配信方式を用いて各記録再生装置に伝送する鍵の種類を、ツリーを構成する特定のグループによって規定されるシステムで共通に利用できるマスターキーとすることも、各記録媒体ごとに固有のメディアキーとすることも可能であり、それぞれに固有のKRBを生成してネットワーク配信、またはメディアを介して配布することにより、キー更新が容易にかつ安全に実行される。

【0336】このため、本発明によれば、映画や音楽などの著作権があるデータの不正な(著作権者の意に反する)複製を防ぐことができる情報記録再生システムを構成することが可能である。

【0337】また、世代管理を行なったマスターキーを使用するシステムにおいて、KRBにより更新された新たな世代のマスターキーを配布する構成とすることにより、KRBとともに暗号化されて配布される更新マスターキーを更新可能なデバイスを特定した固有のキーブロックを構成可能であるので、従来のデバイス単位での認証処理等を実行することなく、安全に更新の必要なデバイスのみが復号可能な暗号化マスターキーを構成して安全に鍵更新が実行できる。

【0338】さらに、本発明の情報記録再生装置および方法によれば、世代管理されたマスターキー、あるいはメディアキーによる暗号化処理のみならず、再生機器制限処理を可能とした暗号処理を実行して記録媒体に格納する構成としている。本構成によって、データを記録媒体に記録する際に、その機器でのみ再生できるようにする(再生機器制限する)場合には機器固有鍵(デバイス固有キー)をデータの暗号鍵に作用させ、そうでない

(再生機器制限しない)場合には機器識別情報(デバイスID)をデータの暗号鍵に作用させて暗号化するようにする。さらに、記録した機器の機器識別情報と、再生機器制限したかしないかのどちらかのモードで記録したかを表す情報(再生機器制限フラグ)を記録媒体に記録しておく構成としたので、データの再生時に、再生機器制限されている場合には機器固有鍵を知っている記録した機器のみがデータを復号でき、再生機器制限されていない場合にはいずれの機器でも記録機器の機器識別情報を用いてデータを復号できるようになる。

【0339】また、各バケットの着信時刻に応じたランダム性のあるデータとして構成されるATSを用いてブロック・データを暗号化するブロックキーを生成する構成としたので、ブロック毎に異なる固有キーを生成することが可能となり、ブロックごとに暗号鍵を変更でき、

暗号解析に対する強度を高めることができる。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【図面の簡単な説明】

【図1】本発明の情報記録再生装置の構成例（その1）を示すブロック図である。

【図2】本発明の情報記録再生装置の構成例（その2）を示すブロック図である。

【図3】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図4】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図5】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図6】本発明の情報記録再生装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図7】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図8】本発明の情報記録再生装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図9】本発明の情報記録再生装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図10】本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図11】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図12】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用されるキー更新ブロック（KRB）の例を示す図である。

【図13】本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（KRB）を使用した配布例と復号処理例を示す図である。

【図14】本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（KRB）を使用した復号処理フローを示す図である。

【図15】本発明の情報記録再生装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。

【図16】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号

化処理を説明するブロック図（その1）である。

【図17】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その2）である。

【図18】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理を説明するフローチャートである。

【図19】本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

【図20】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるタイトル固有キーの生成処理フローを示す図である。

【図21】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録時のタイトル固有キーの生成処理例を示す図である。

【図22】本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

【図23】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

【図24】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理を説明するフローチャートである。

【図25】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理における再生可能判定処理の詳細を示すフローチャートである。

【図26】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ最盛時のタイトル固有キーの生成処理フローを示す図である。

【図27】本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（KRB）を使用した配布例と復号処理例を示す図である。

【図28】本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（KRB）を使用した復号処理フローを示す図である。

【図29】本発明の情報記録再生装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。

【図30】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その1）である。

【図31】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その2）である。

【図32】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理を説明するフローチャートである。

【図33】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理時の暗号化処理を説明するブロック図である。

【図34】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理を説明するフローチャートである。

【図35】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

【図36】本発明の情報記録再生装置において、外部からKRBを通信手段等を介して受信し、記録媒体に格納する構成とした記録再生装置構成を示すブロック図である。

【図37】本発明の情報記録再生装置において、外部からKRBを通信手段等を介して受信し、記録媒体に格納する処理について示すブロック図である。

【図38】本発明の情報記録再生装置において、外部からKRBを通信手段等を介して受信し、記録媒体に格納する処理フローを示すブロック図である。

【図39】本発明の情報記録再生装置において、外部からKRBを通信手段等を介して受信し、記録媒体に格納する処理を説明する図である。

【図40】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図41】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

【図42】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【図43】本発明の情報記録再生装置において使用される情報記録媒体を製造する製造装置の構成を示すブロック図である。

【図44】本発明の情報記録再生装置において使用される情報記録媒体を製造する製造処理の処理フローを示す図である。

【図45】本発明の情報記録再生装置において使用されるキー更新ブロック(KRB)のフォーマット例を示す図である。

【図46】本発明の情報記録再生装置において使用されるキー更新ブロック(KRB)のタグの構成を説明する図である。

【符号の説明】

100, 200 記録再生装置

110 バス

120 入出力I/F

130 MPEGコーデック

140 入出力I/F

141 A/D, D/Aコンバータ

150 暗号処理手段

160 ROM

170 CPU

180 メモリ

190 ドライブ

195 記録媒体

210 記録媒体I/F

300 TS処理手段

600, 607 端子

602 ビットストリームパーサー

603 PLL

604 タイムスタンプ発生回路

605 ブロックシード付加回路

606 スムージングバッファ

800, 806 端子

801 ブロックシード分離回路

802 出力制御回路

803 比較器

804 タイミング発生回路

805 27MHzクロック

901, 904, 913 端子

902 MPEGビデオエンコーダ

903 ビデオストリームバッファ

905 MPEGオーディオエンコーダ

906 オーディオストリームバッファ

908 多重化スケジューラ

909 トランスポートパケット符号化器

910 到着タイムスタンプ計算手段

911 ブロックシード付加回路

912 スムージングバッファ

976 スイッチ

4201 バス

4202 CPU

4203 ROM

4204 RAM

4205 ハードディスク

4206 出力部

4207 入力部

4208 通信部

4209 ドライブ

4210 リムーバブル記録媒体

4211 入出力インタフェース

4300 ディスク製造装置

4301 制御部

4302 メモリ

4303 記録媒体I/F

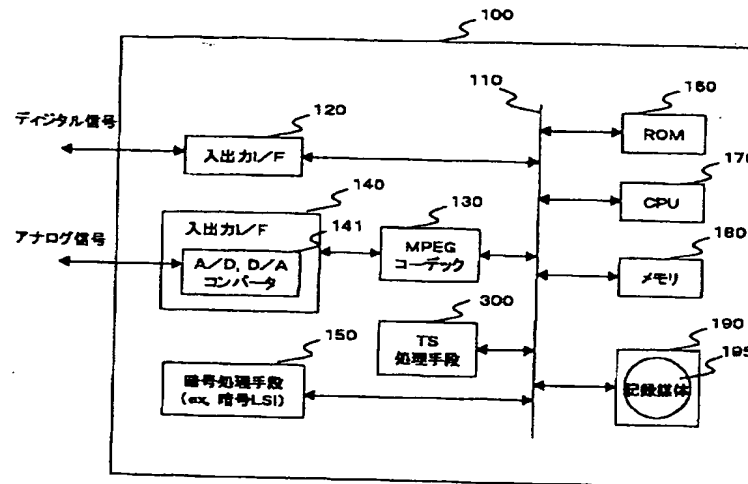
4304 入出力I/F

4305 バス

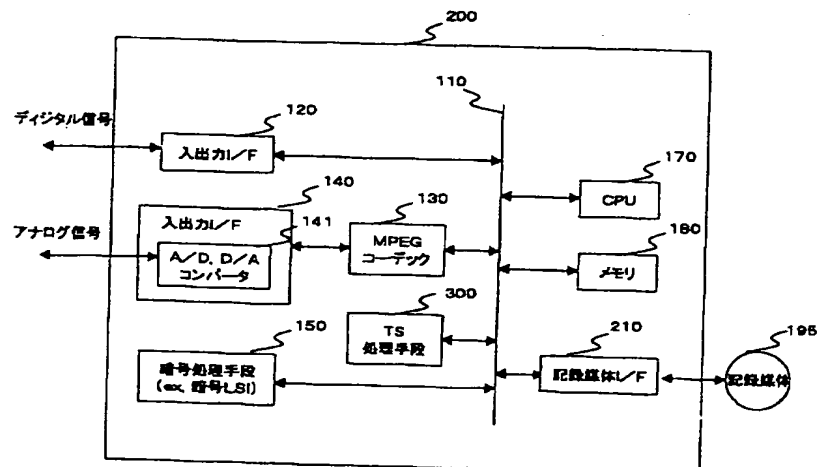
4350 記録媒体  
 4501 バージョン  
 4502 デブス  
 4503 データポインタ  
 4504 タグポインタ

4505 署名ポインタ  
 4506 データ部  
 4507 タグ部  
 4508 署名

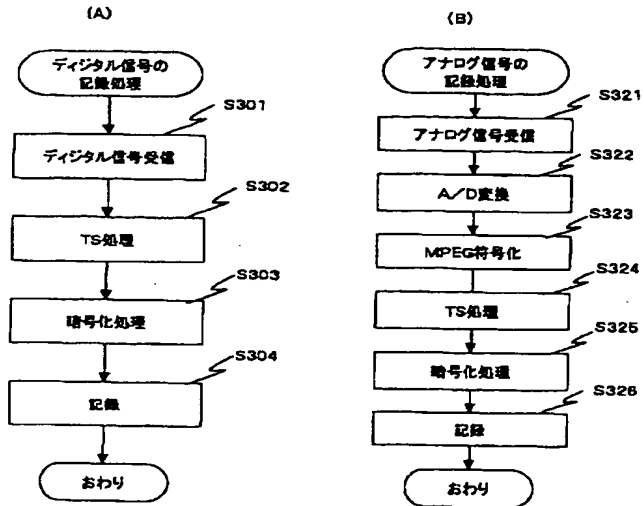
【図1】



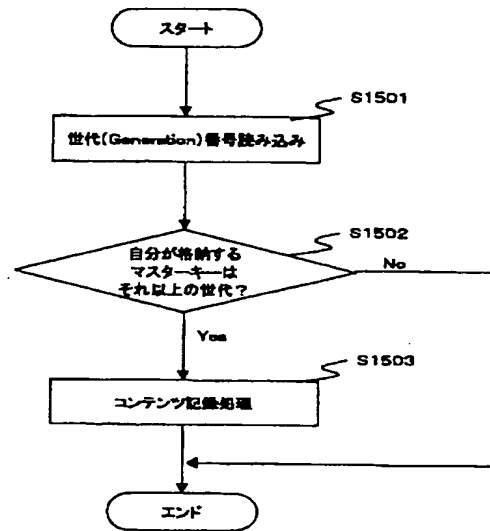
【図2】



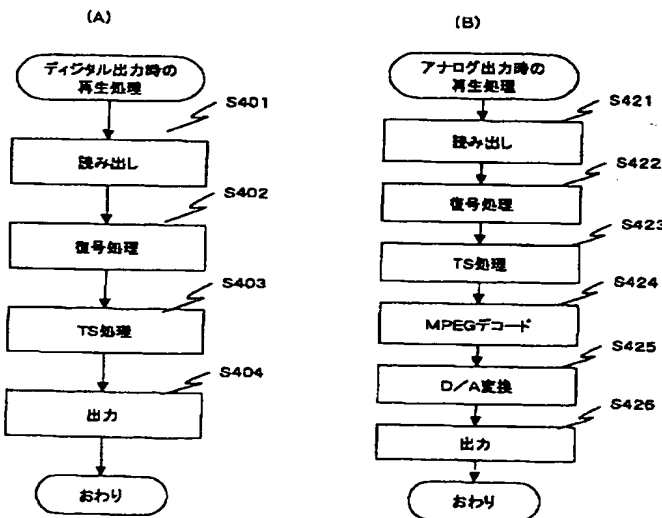
【図3】



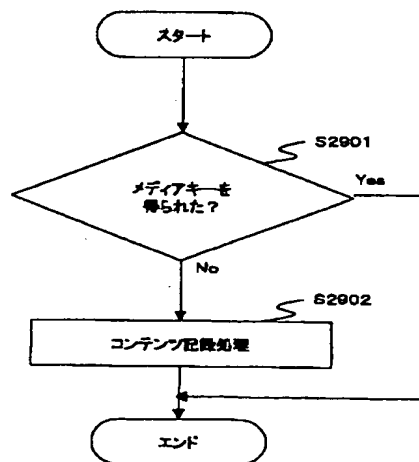
【図15】



【図4】

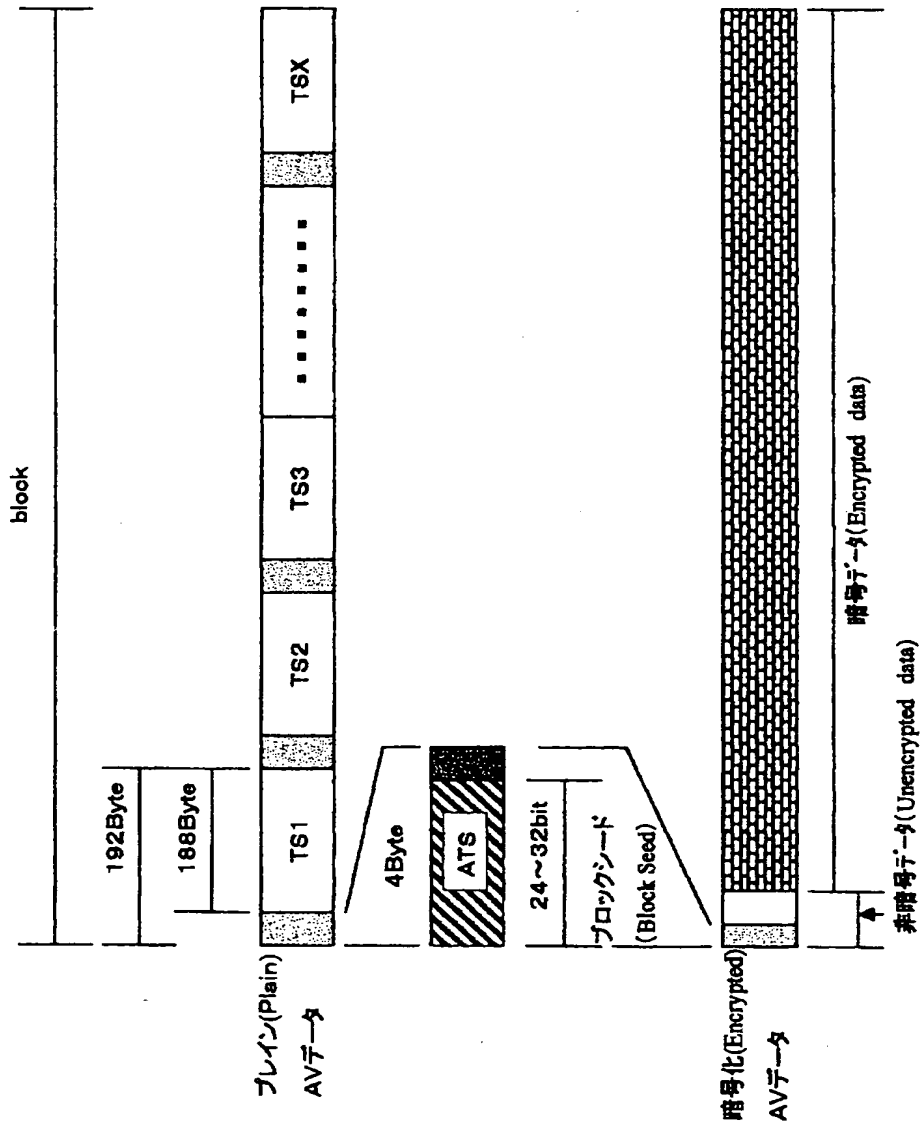


【図29】

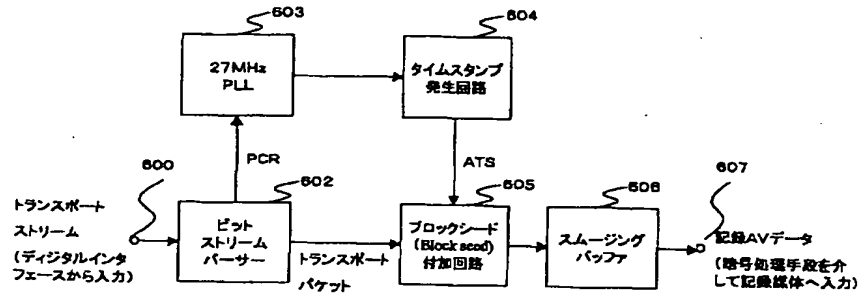




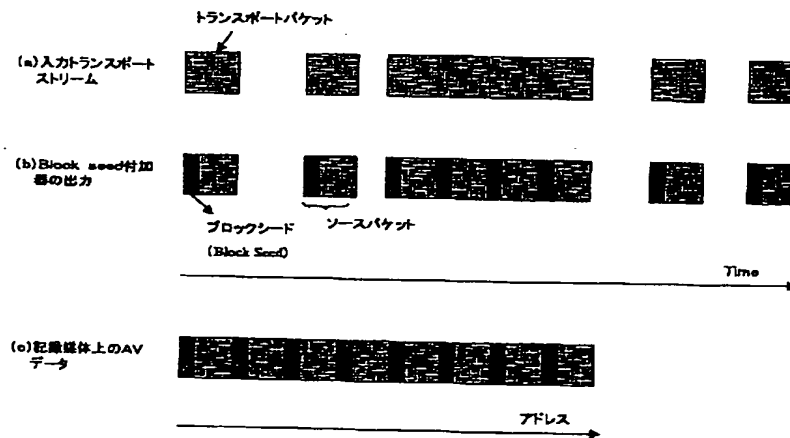
【図5】



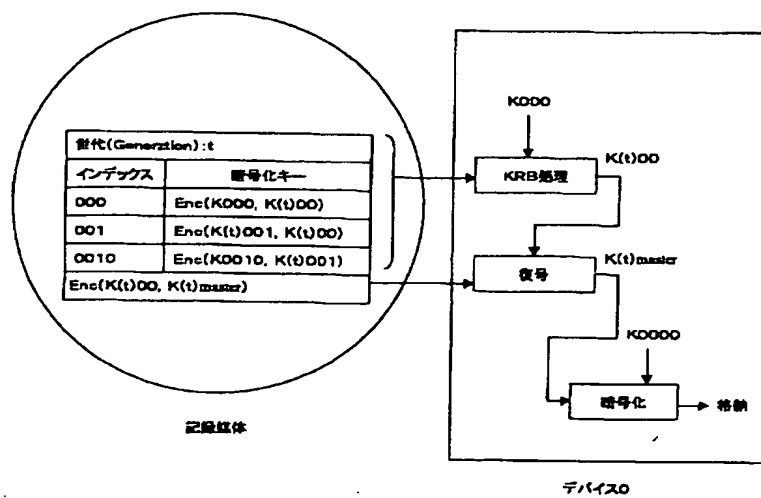
【図6】



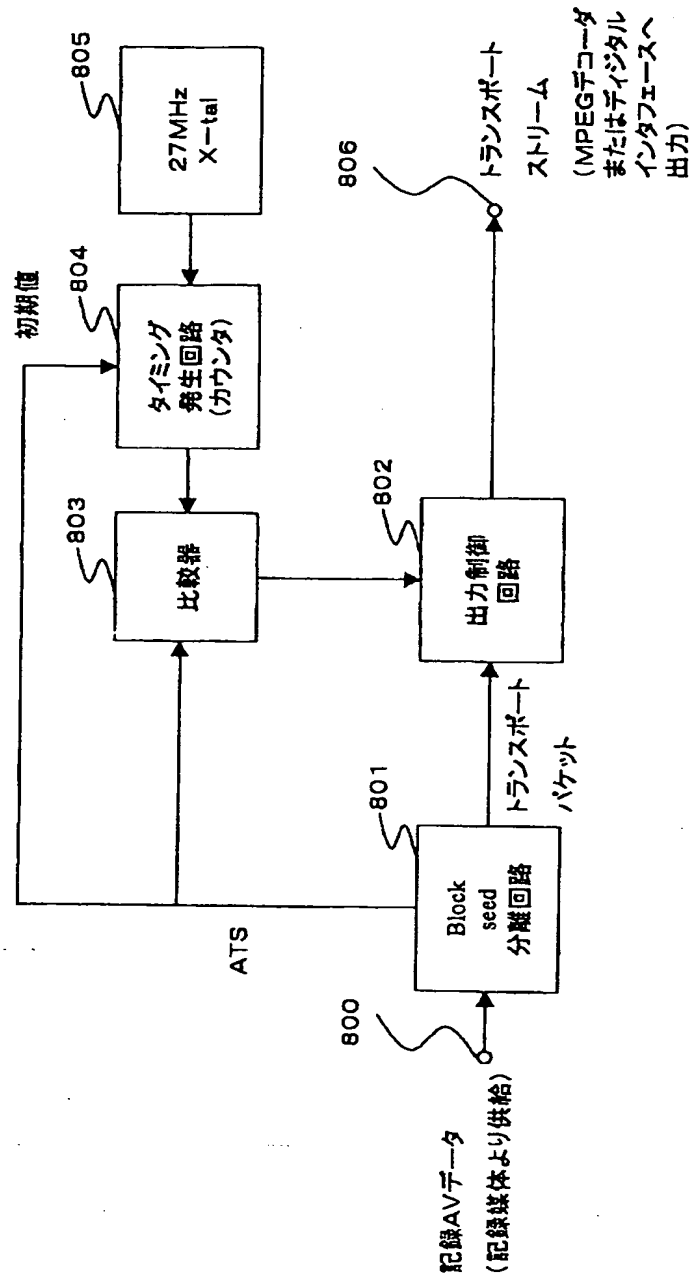
【図7】



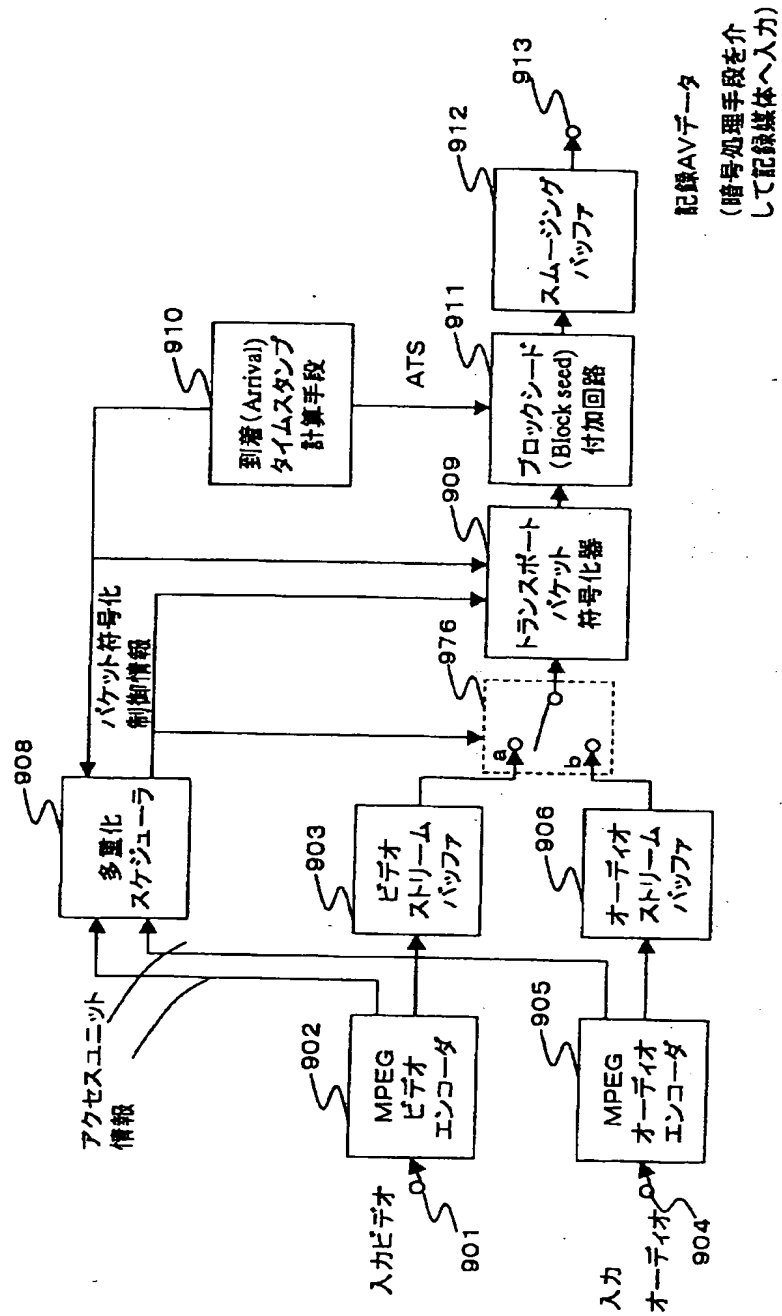
【図13】



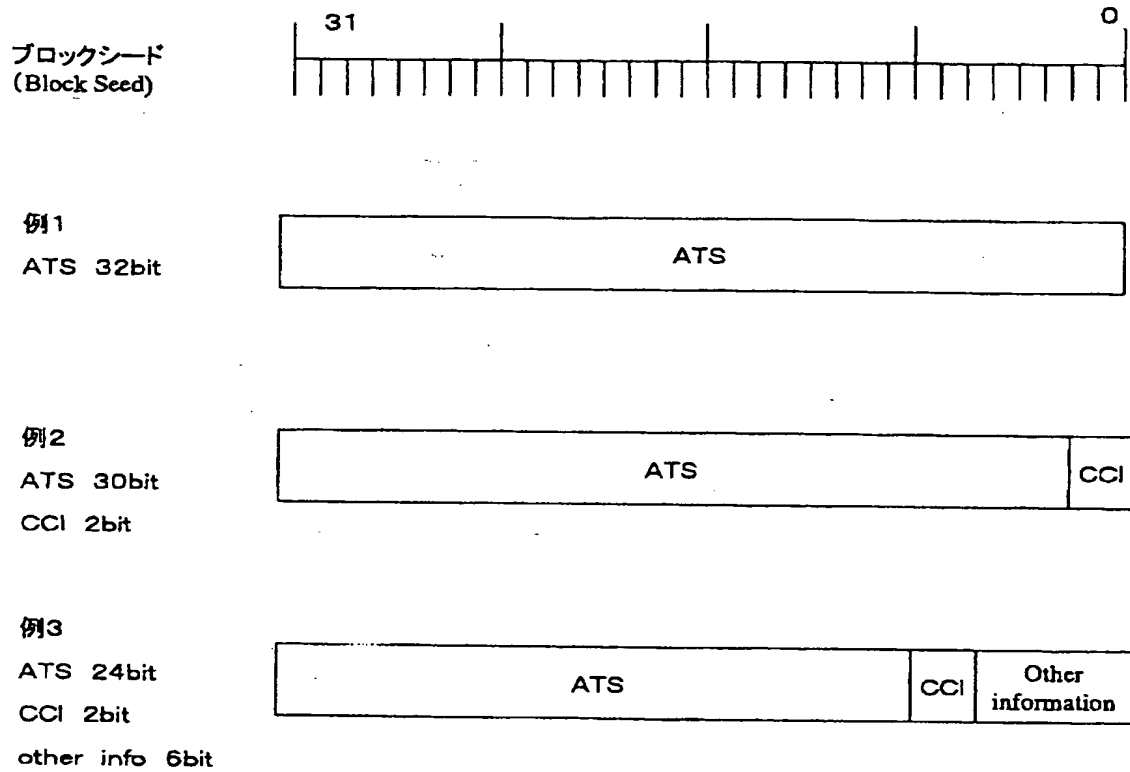
【図8】



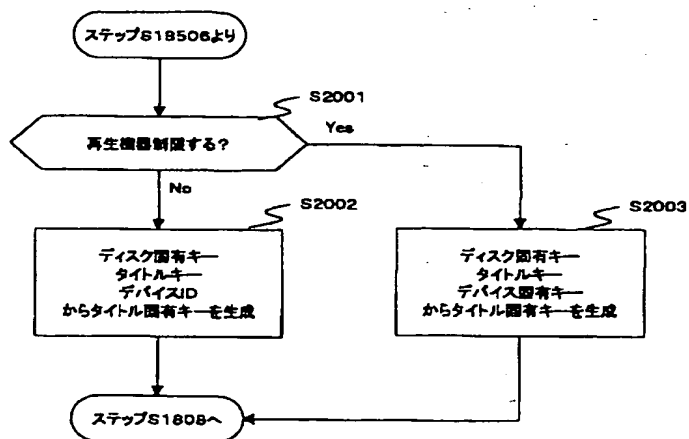
【図9】



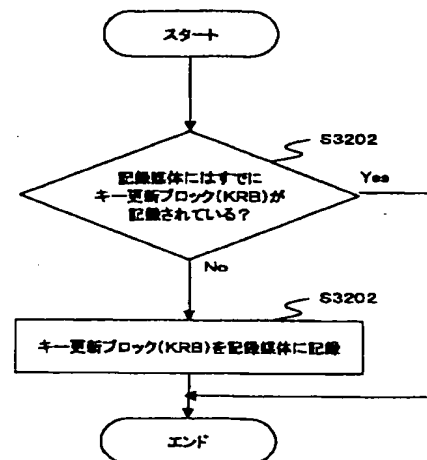
【図10】



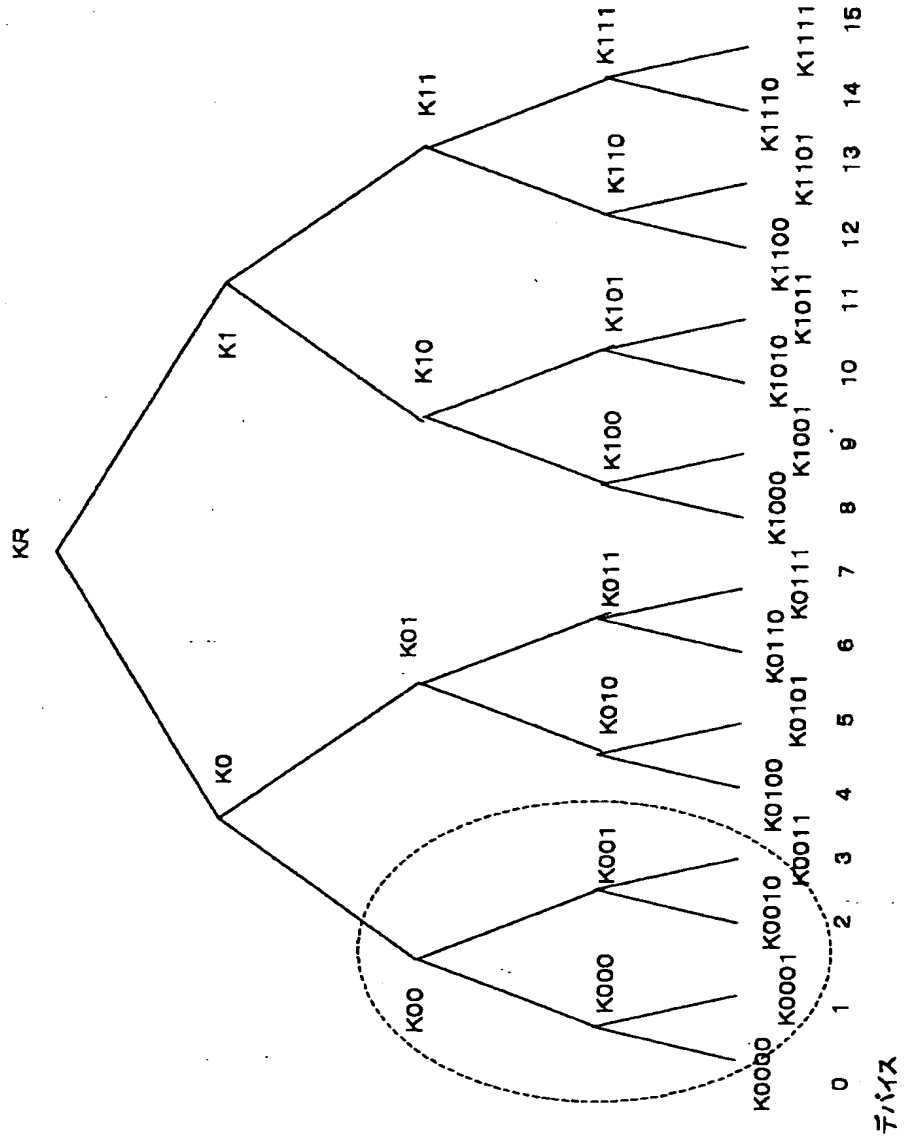
【図20】



【図38】



【図11】



【図12】

## (A) キー更新ブロック(KRB:Key Renewal Block) 例1

デバイス0, 1, 2にt時点でのルートキー $K(t)R$ を送付

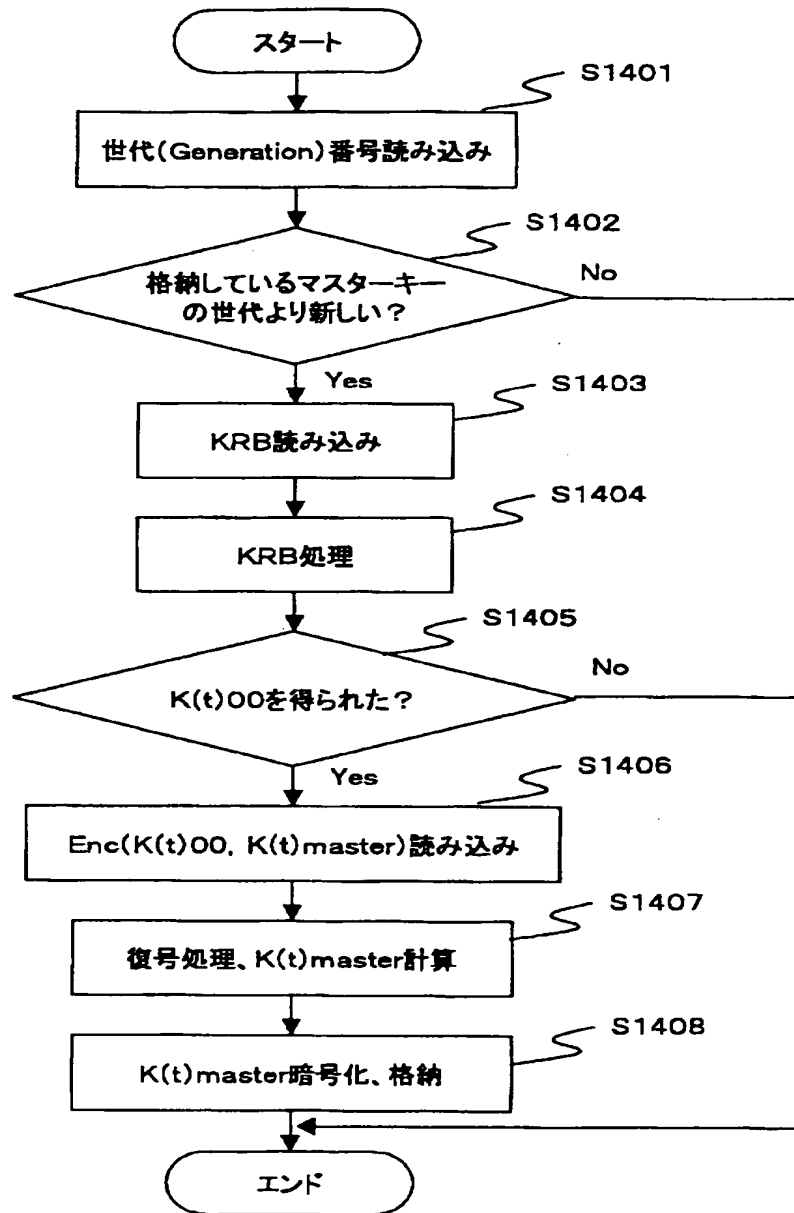
世代(Generztion):t	
インデックス	暗号化キー
0	$Enc(K(t)0, K(t)R)$
00	$Enc(K(t)00, K(t)0)$
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

## (B) キー更新ブロック(KRB:Key Renewal Block) 例2

デバイス0, 1, 2にt時点でのルートキー $K(t)R$ を送付

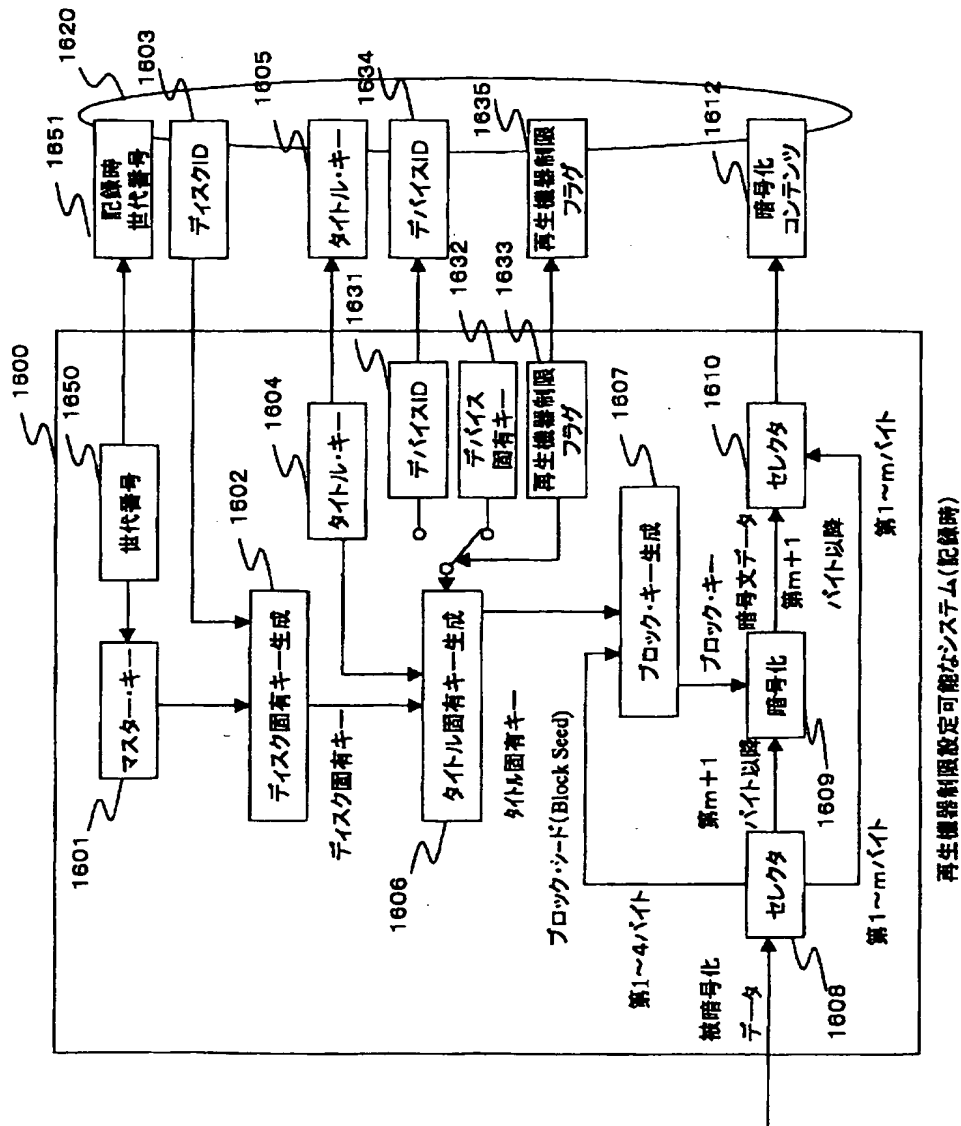
世代(Generztion):t	
インデックス	暗号化キー
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

【図14】

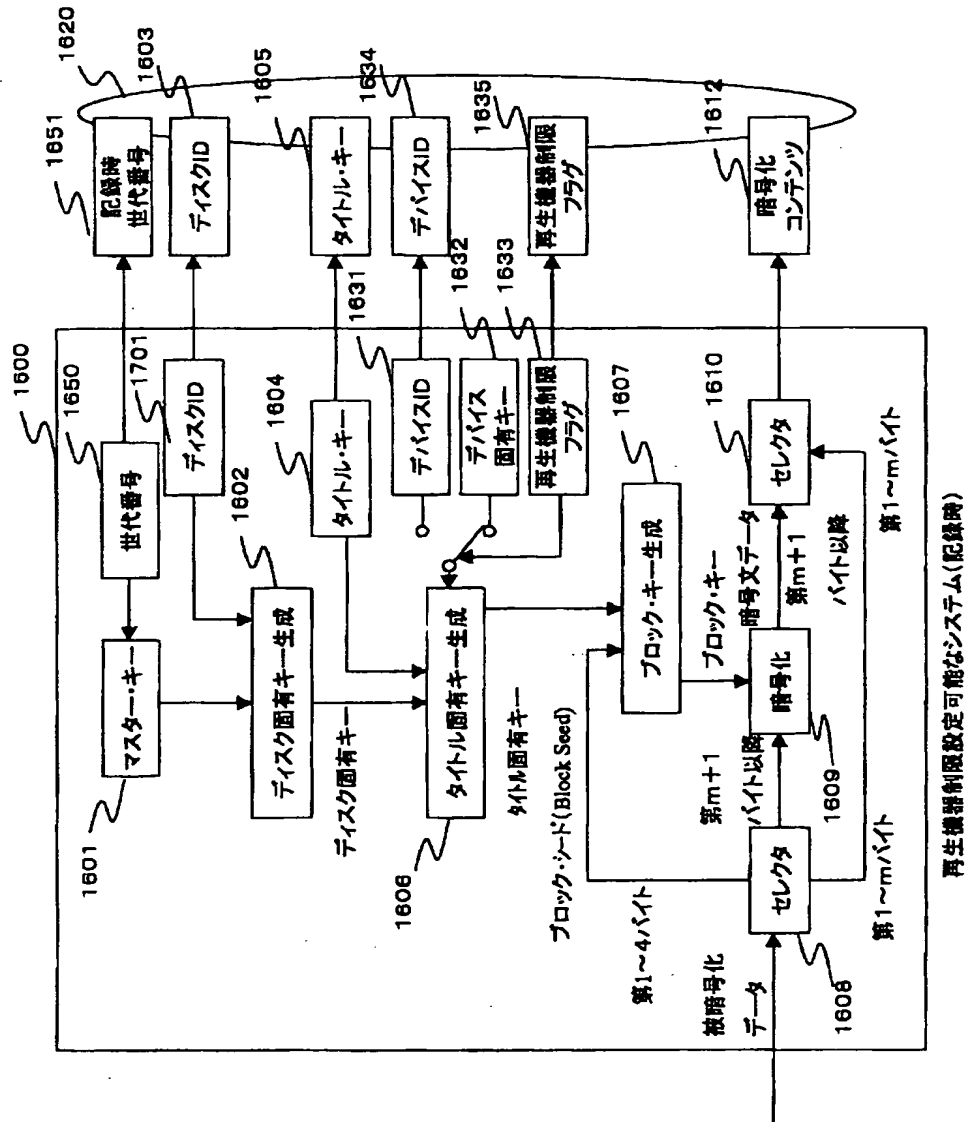




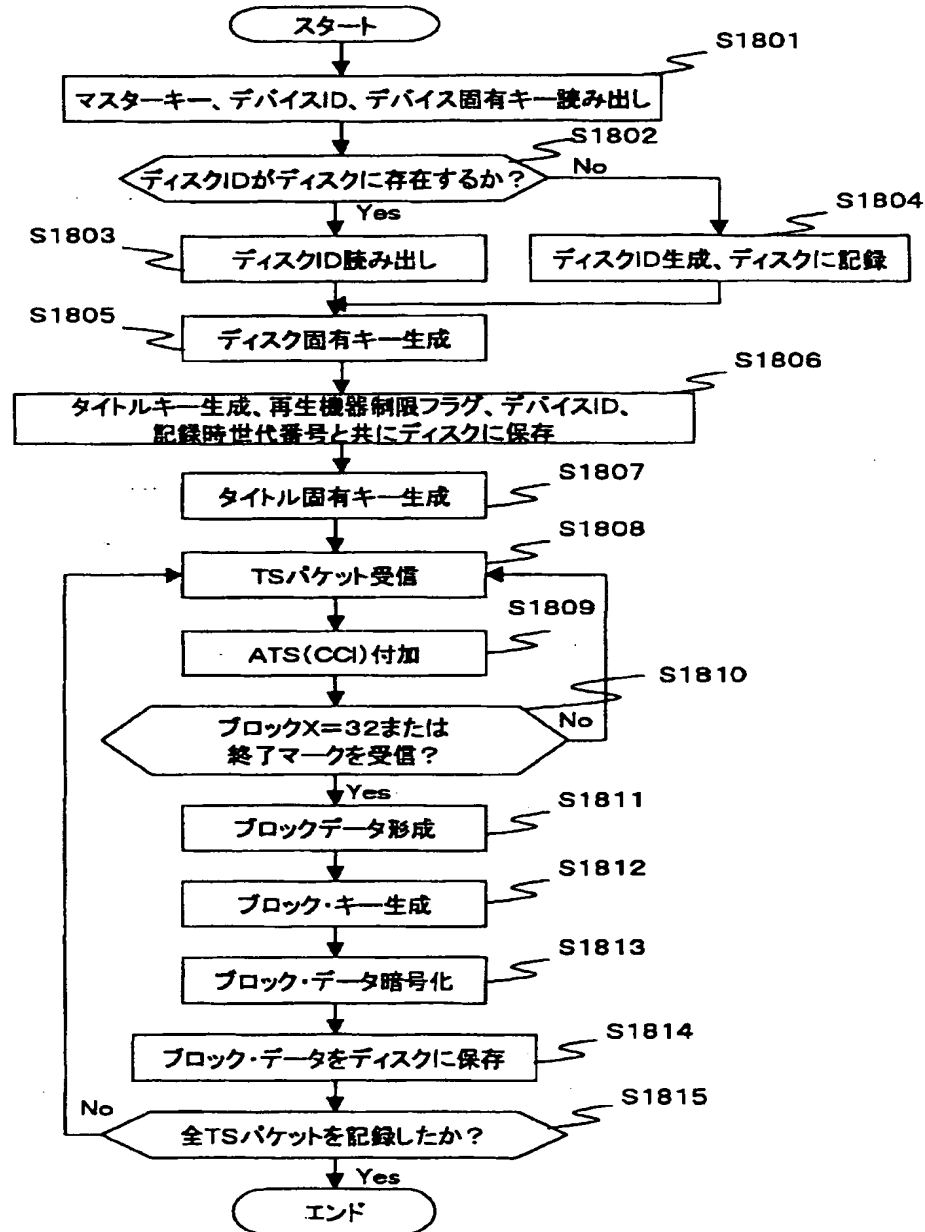
【図16】



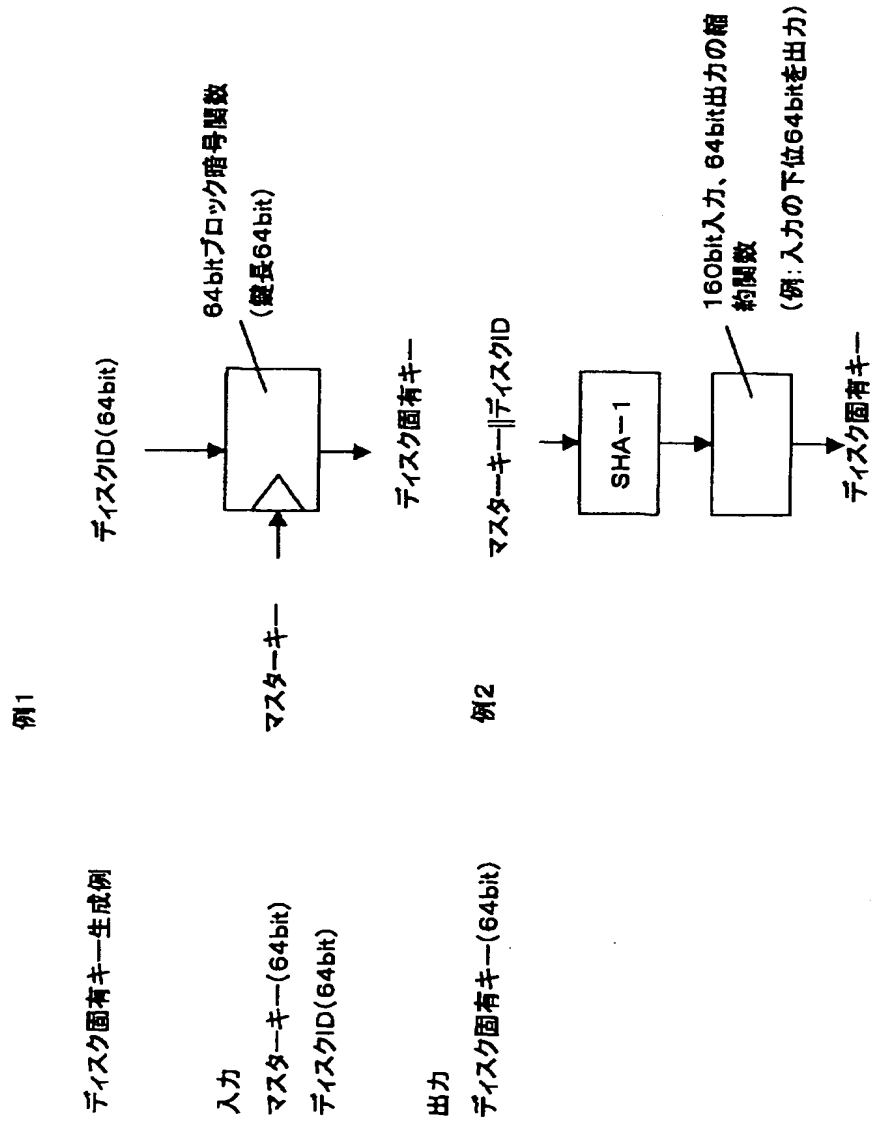
【図17】



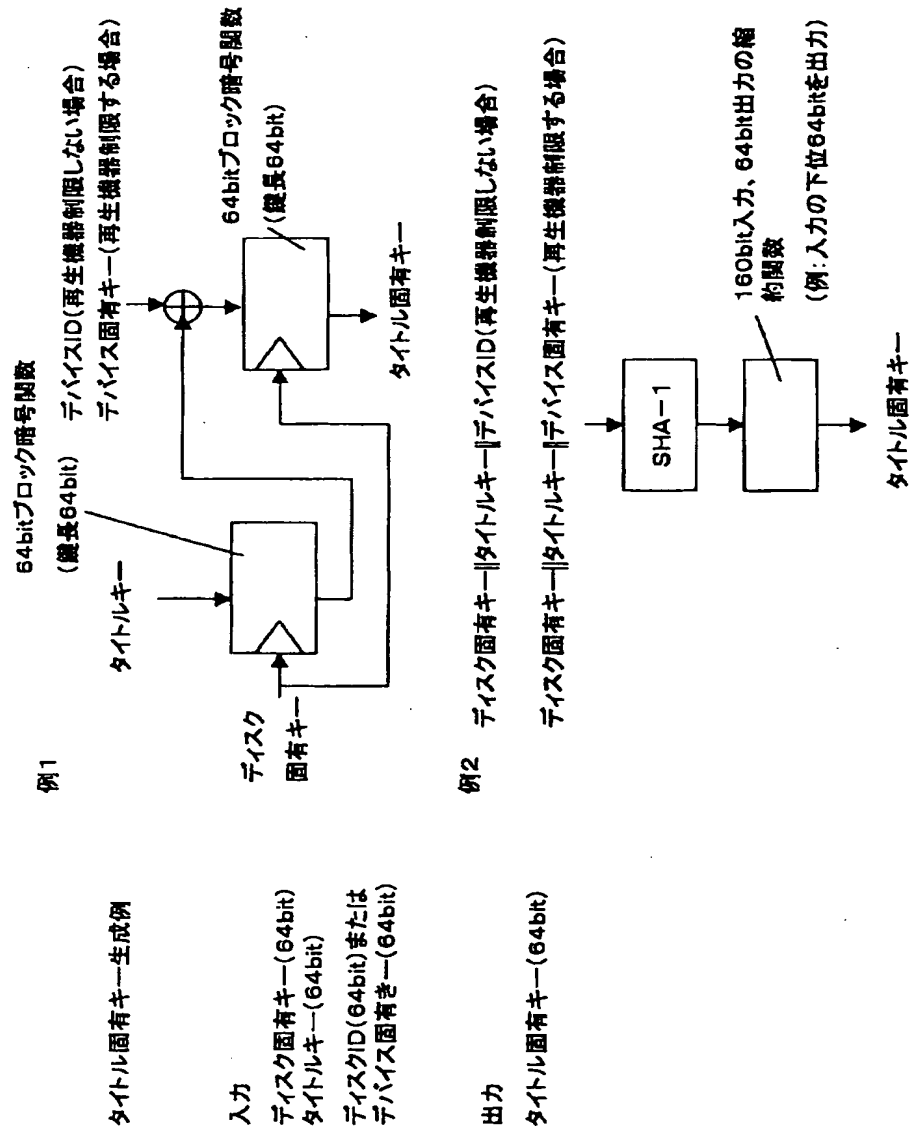
【図18】



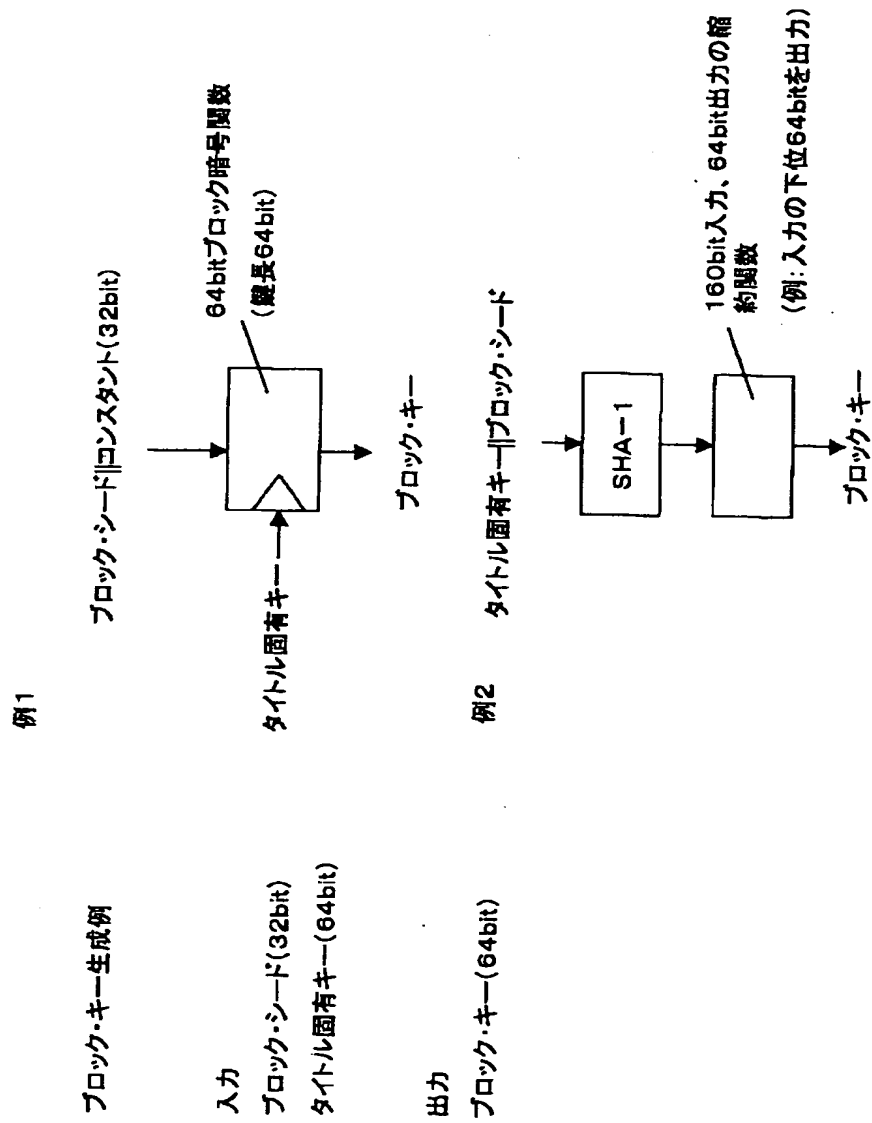
【図19】



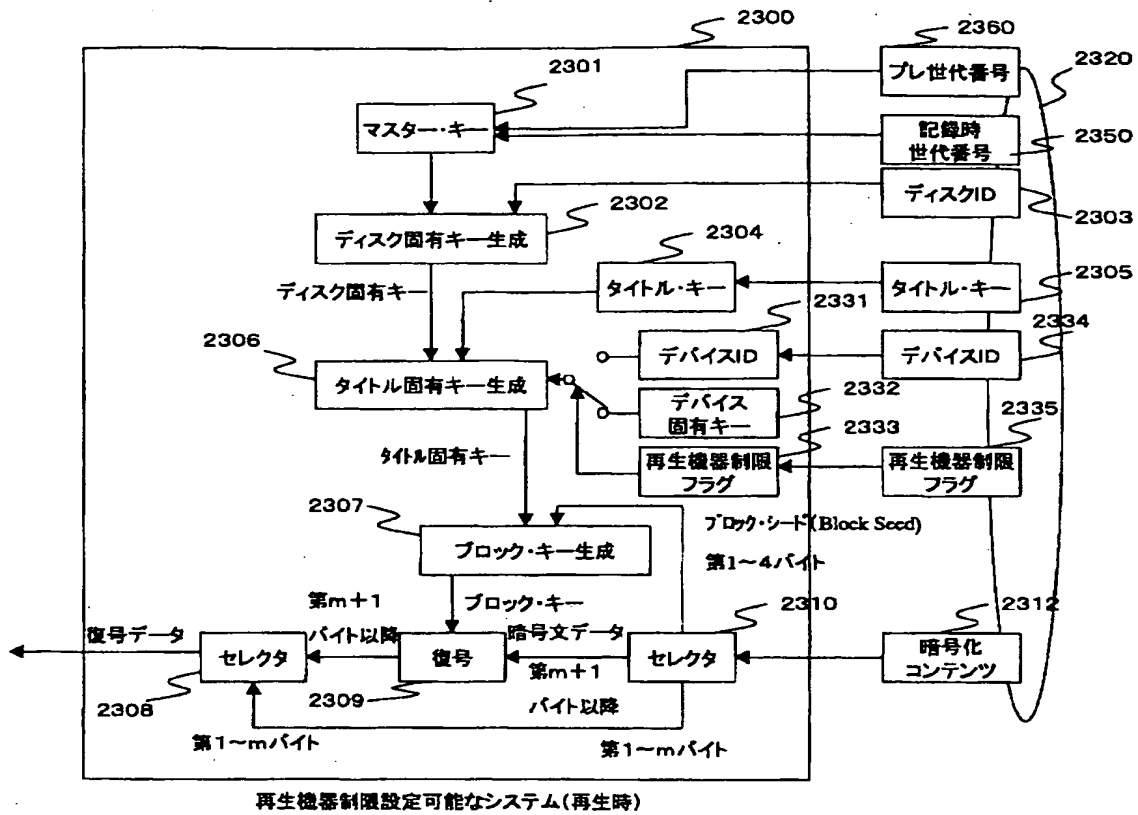
【図21】



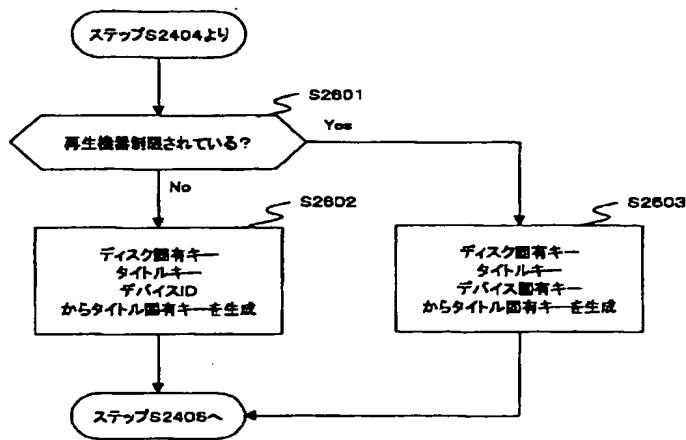
【図22】



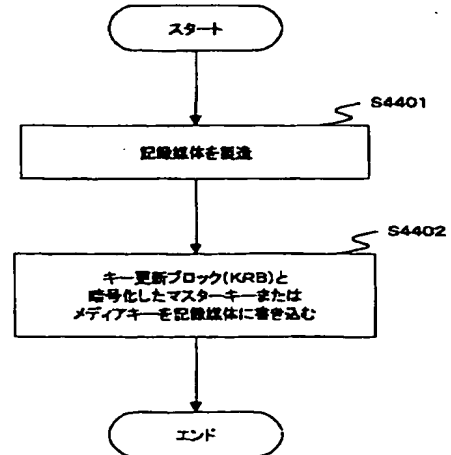
【図23】



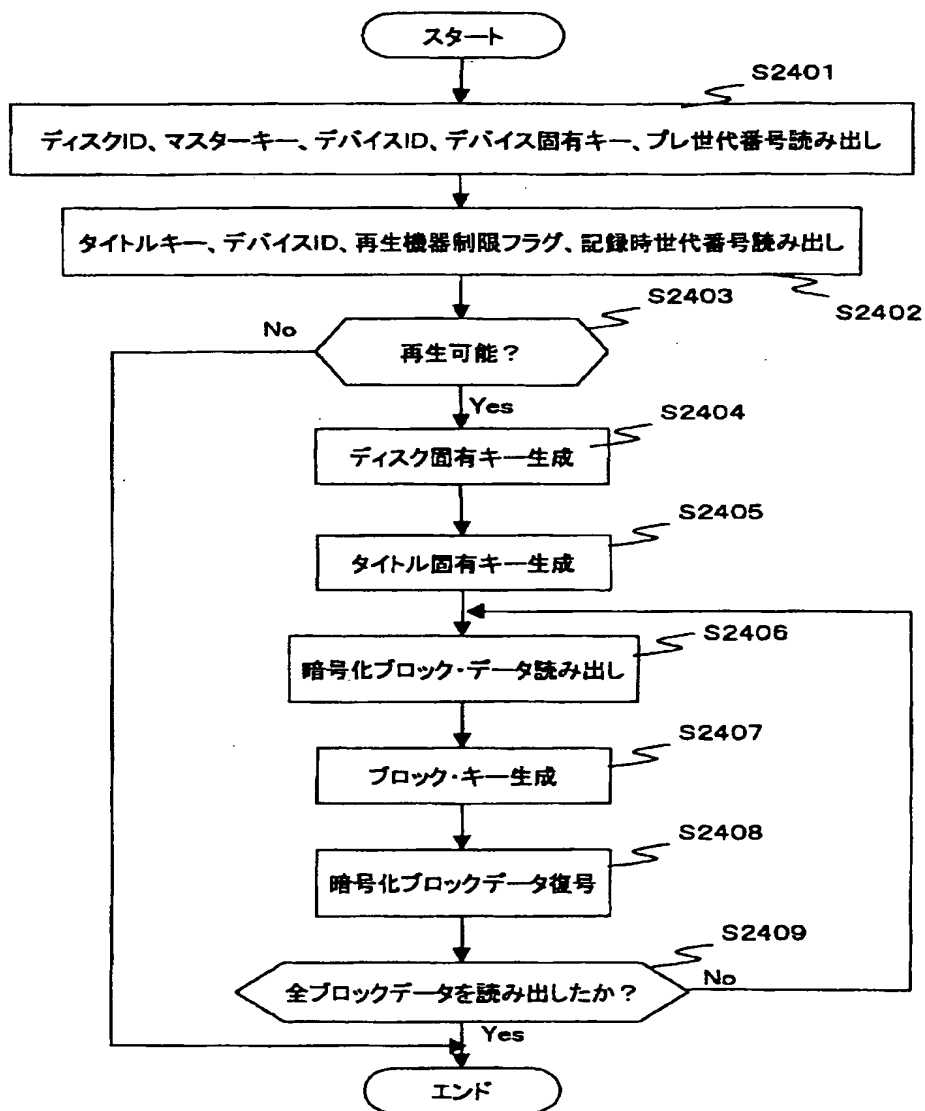
【図26】



【図44】

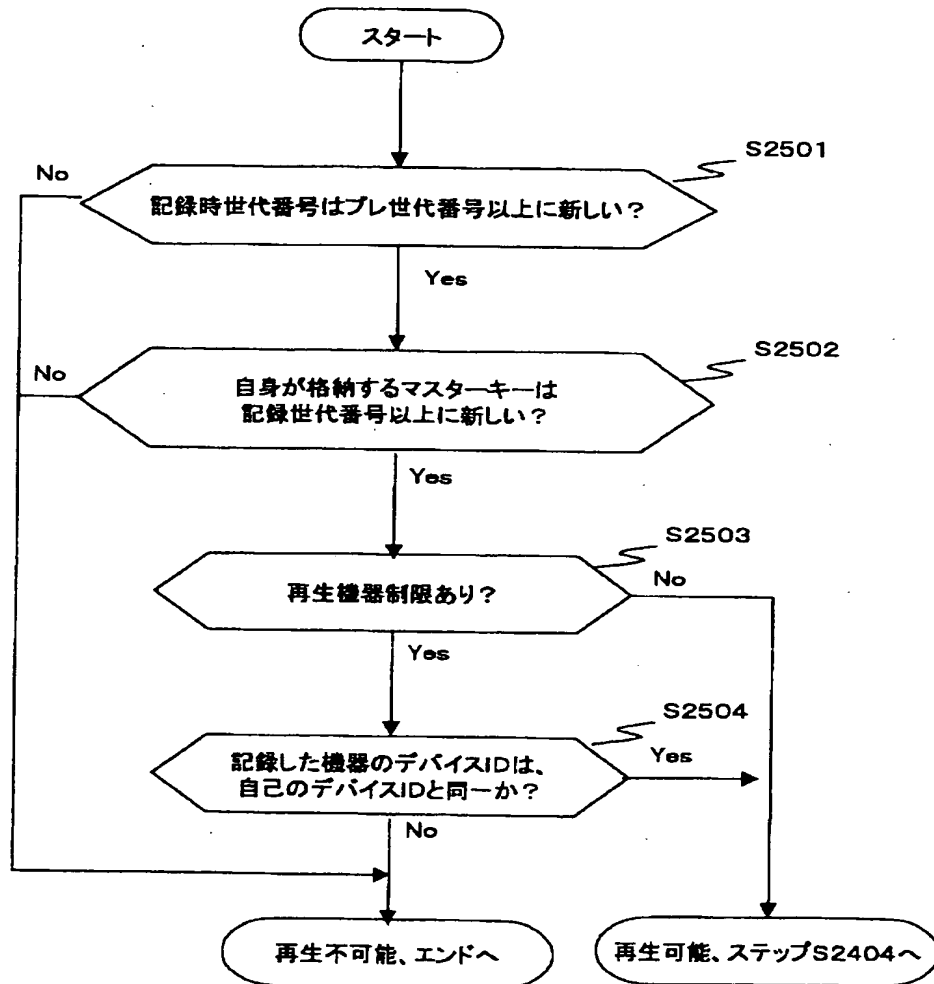


【図24】

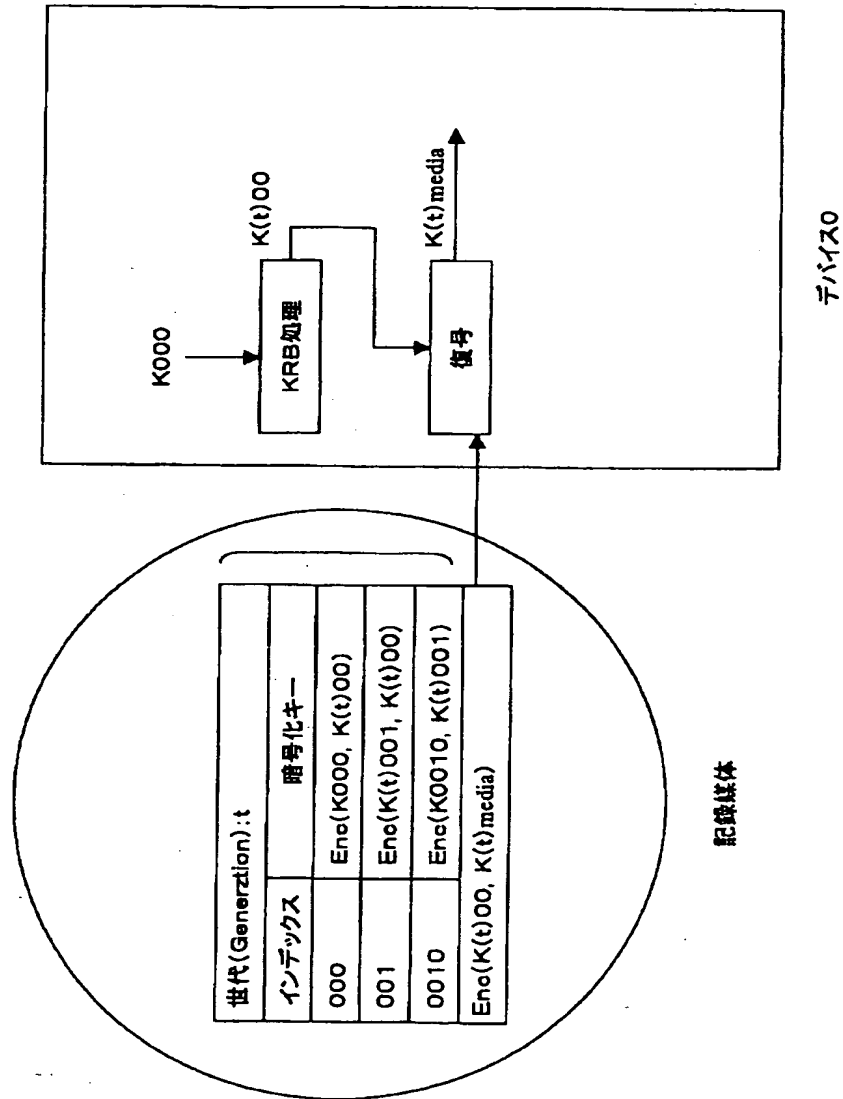




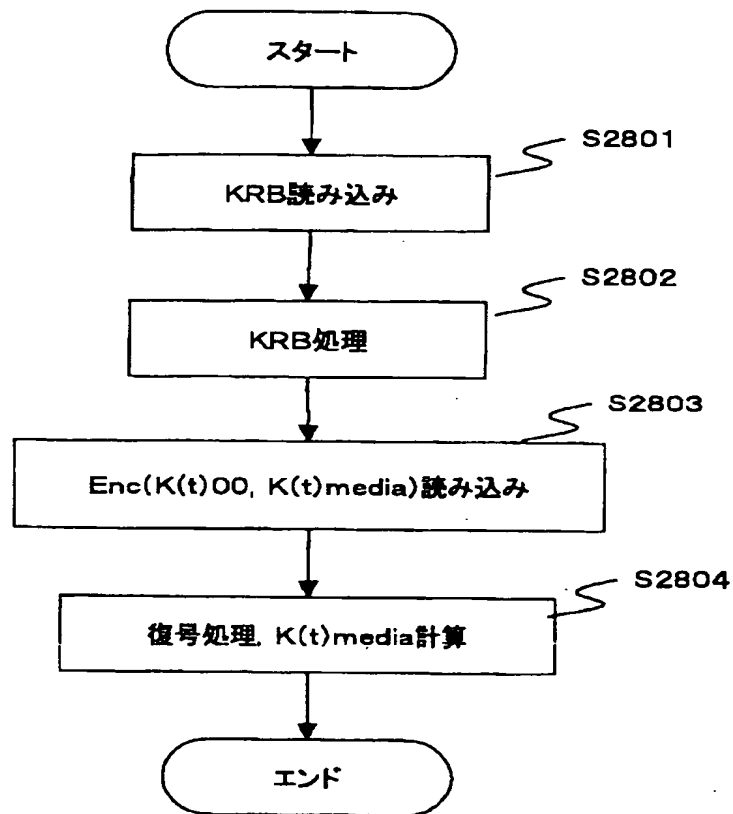
【図25】



【図27】



【図28】



【図35】

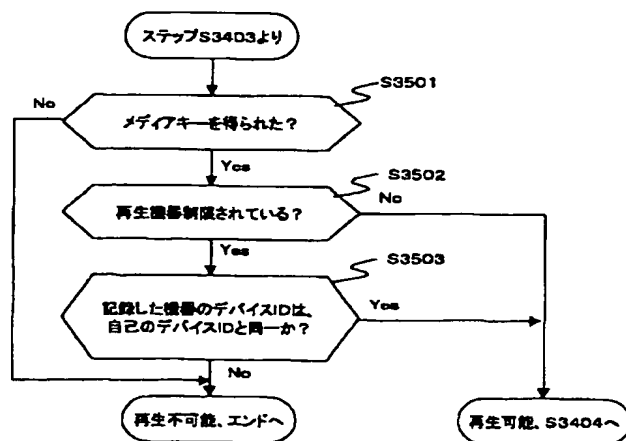


Figure 1 is a block diagram of a reproduction system (3000). The system is divided into two main sections: 3001 (Media Key Management) and 3020 (Data Encryption/Decryption).

**Section 3001 (Media Key Management):**

- メディアキー (Media Key):** The input key.
- ディスク固有キー生成 (Disk Unique Key Generation):** Generates a disk unique key from the media key.
- タイトル固有キー生成 (Title Unique Key Generation):** Generates a title unique key from the disk unique key.
- タイトル・キー (Title Key):** The output key from the title unique key generation.
- ディスクID (Disk ID):** A unique identifier for the disk.
- デバイスID (Device ID):** A unique identifier for the device.
- 再生機器制限フラグ (Reproduction Machine Restriction Flag):** A flag indicating reproduction restrictions.

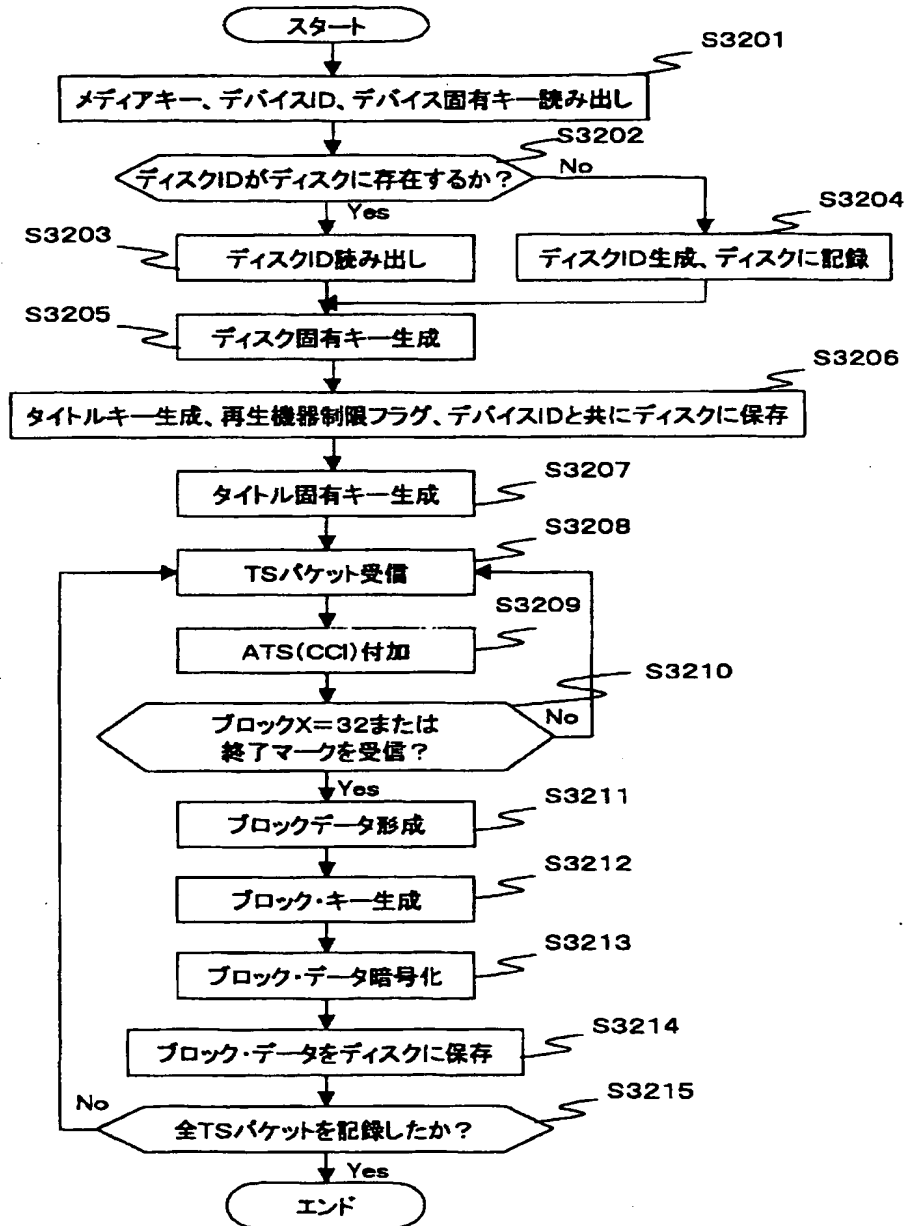
**Section 3020 (Data Encryption/Decryption):**

- 暗号化データ (Encrypted Data):** The input data to be encrypted.
- 暗号化 (Encryption):** The process of encrypting the data using the title key.
- 暗号文データ (Cipher Text Data):** The output of the encryption process.
- セレクタ (Selector):** A component that selects the appropriate key for encryption/decryption.
- ブロック・キー生成 (Block Key Generation):** Generates a block key from the title key.
- ブロック・キー (Block Key):** The output key from the block key generation.
- 再生機器制限フラグ (Reproduction Machine Restriction Flag):** A flag indicating reproduction restrictions.
- 暗号化 (Encryption):** The process of encrypting the data using the block key.
- 暗号文データ (Cipher Text Data):** The output of the encryption process.
- セレクタ (Selector):** A component that selects the appropriate key for encryption/decryption.

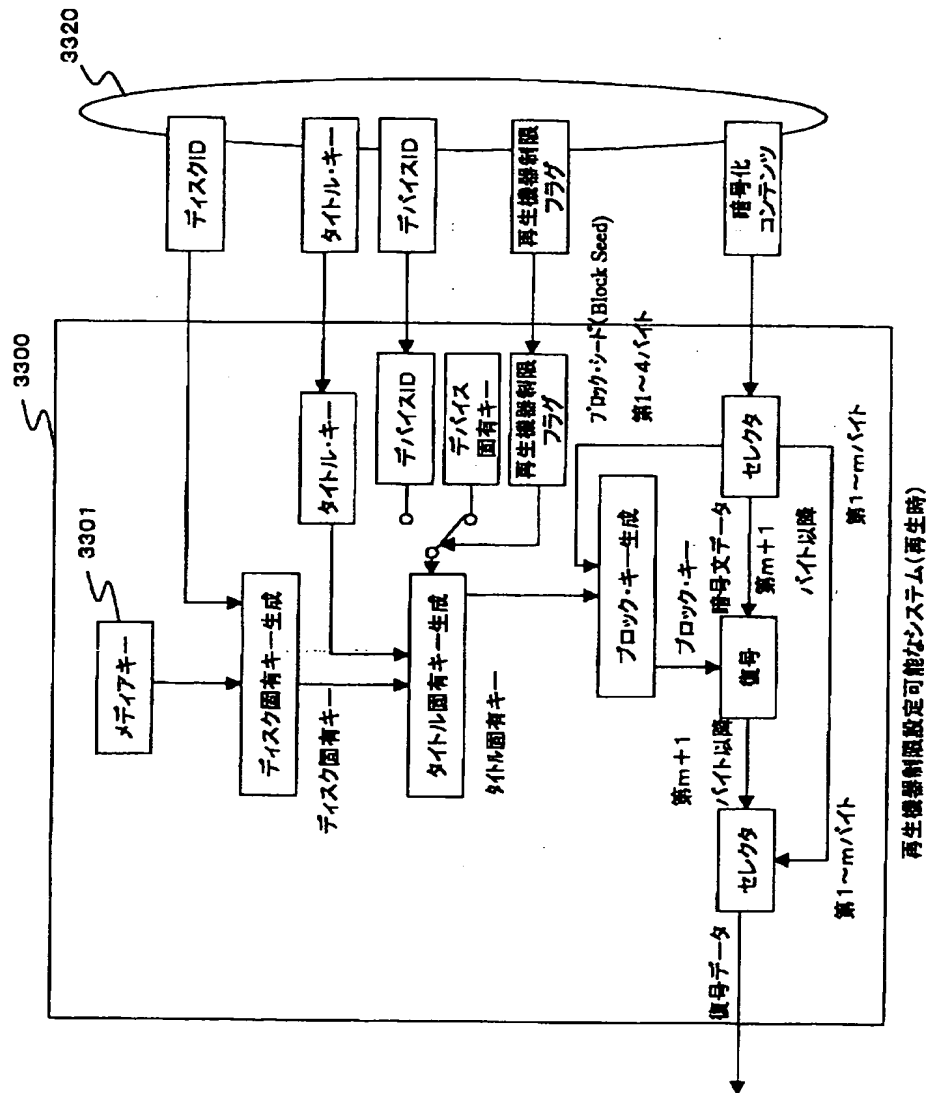
The diagram shows the flow of data and keys between these components, with labels indicating the specific keys and flags used in the process.



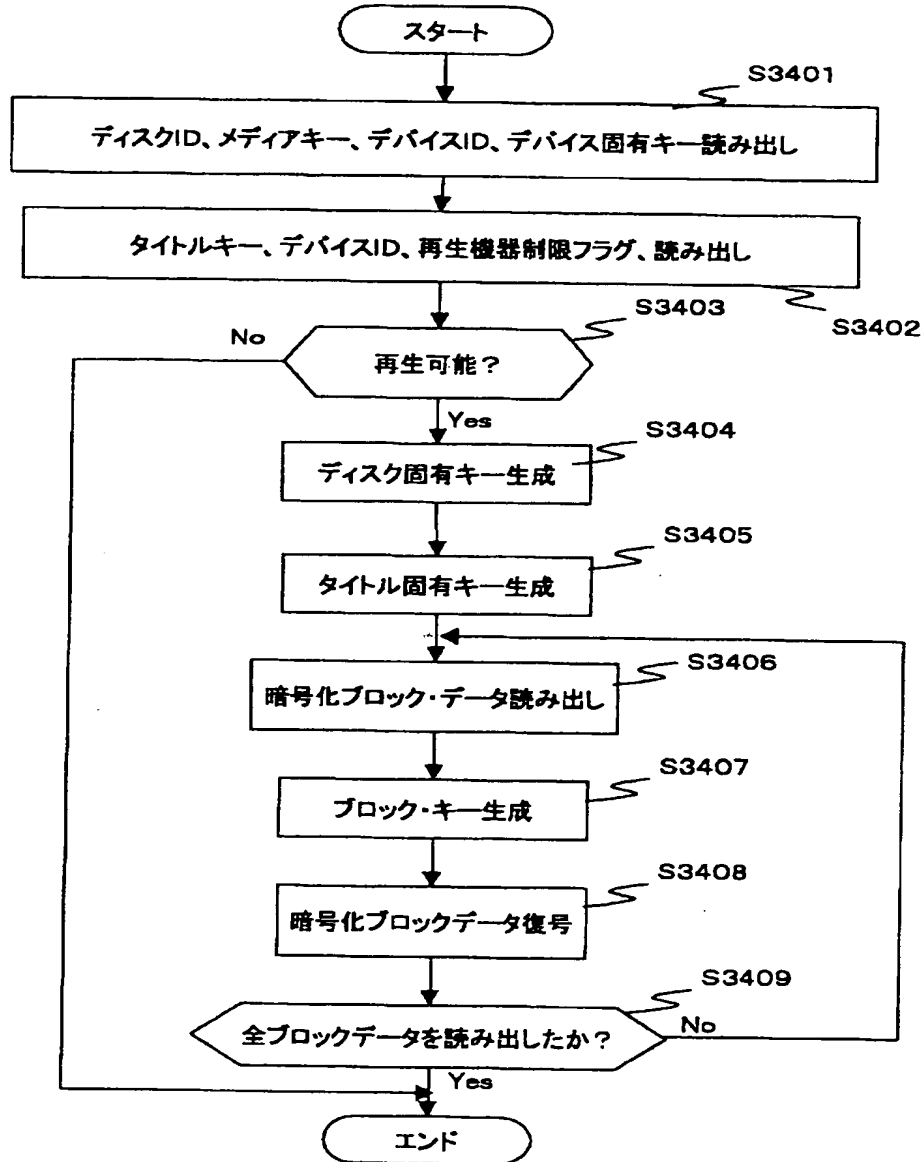
【図32】



【図33】

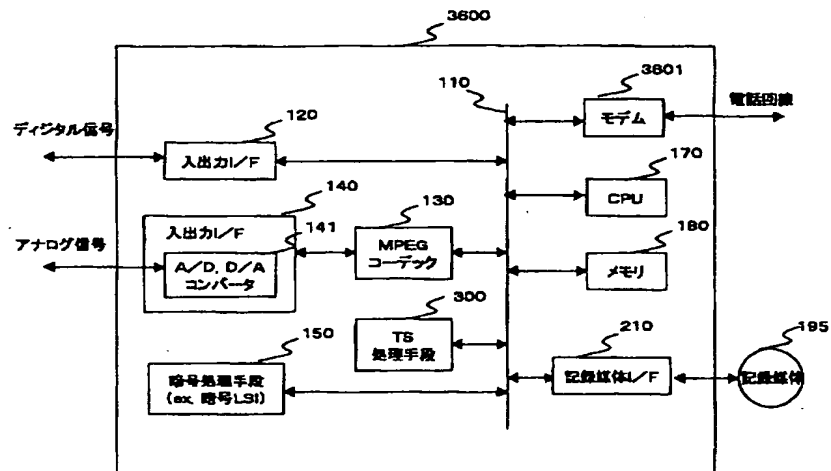


【図34】

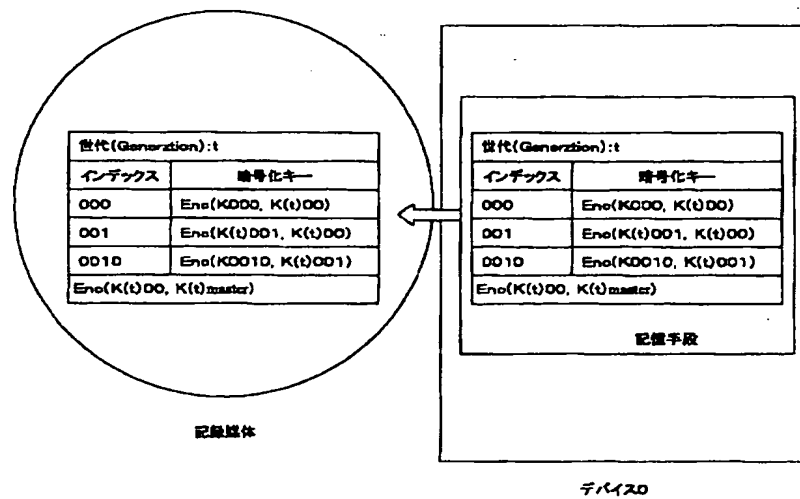




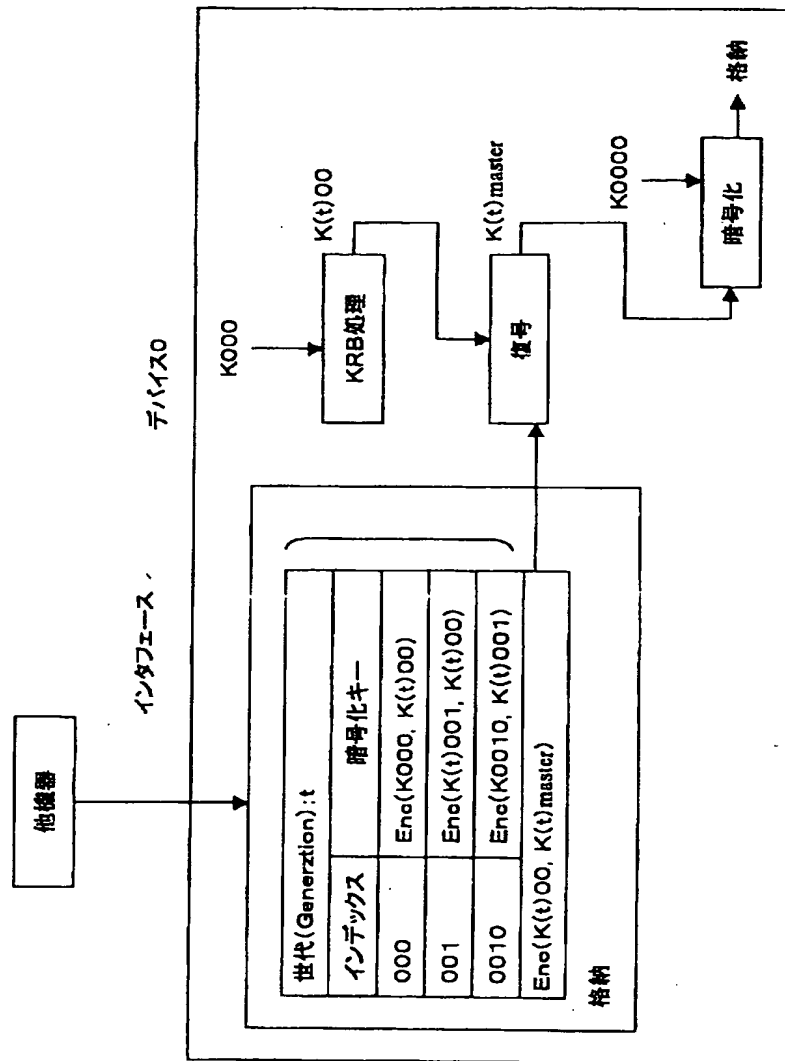
【図36】



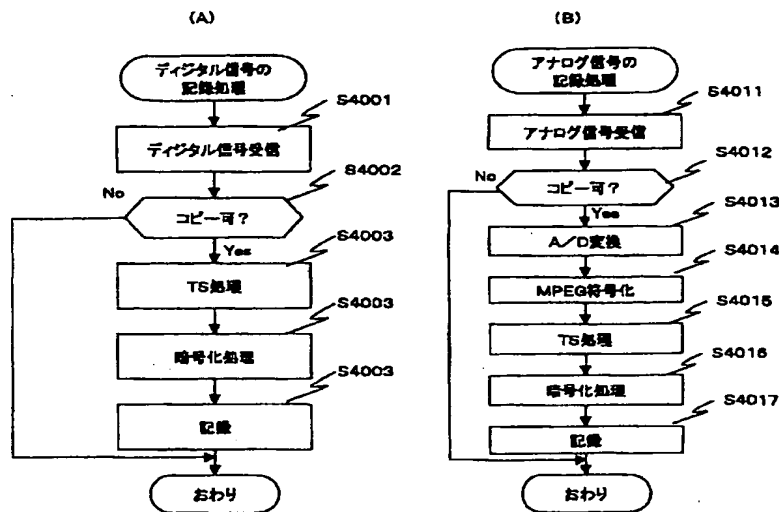
【図39】



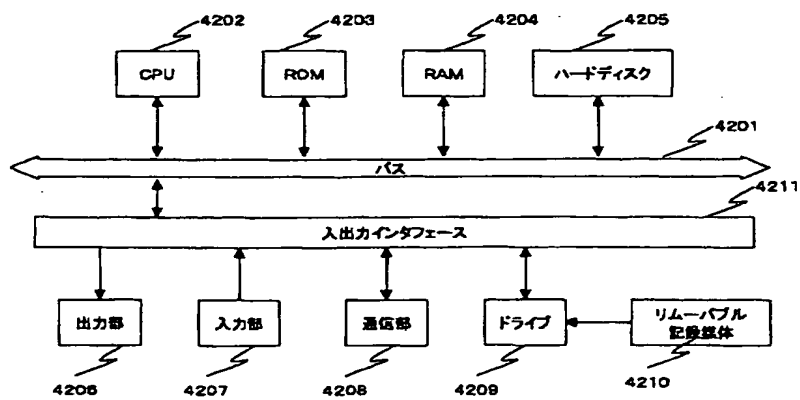
【図37】



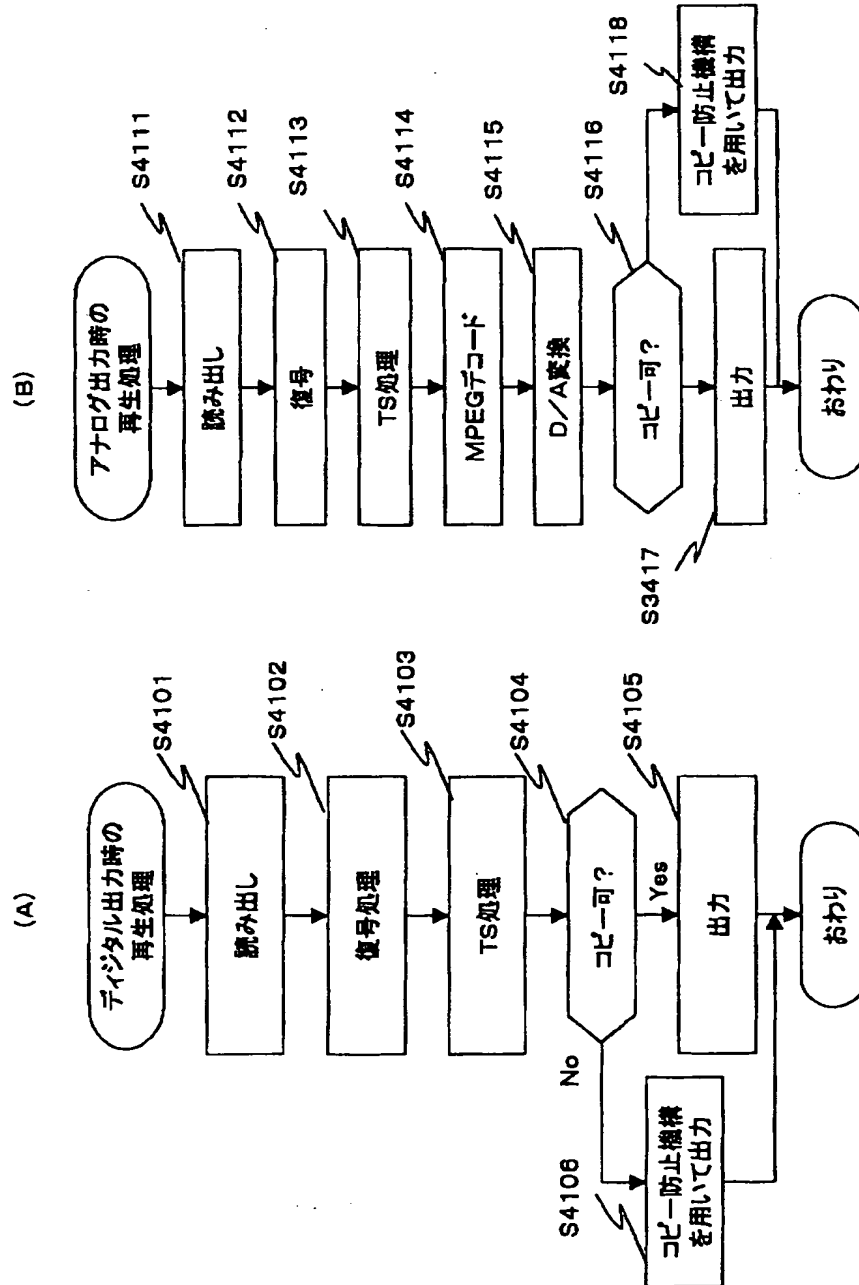
【図40】



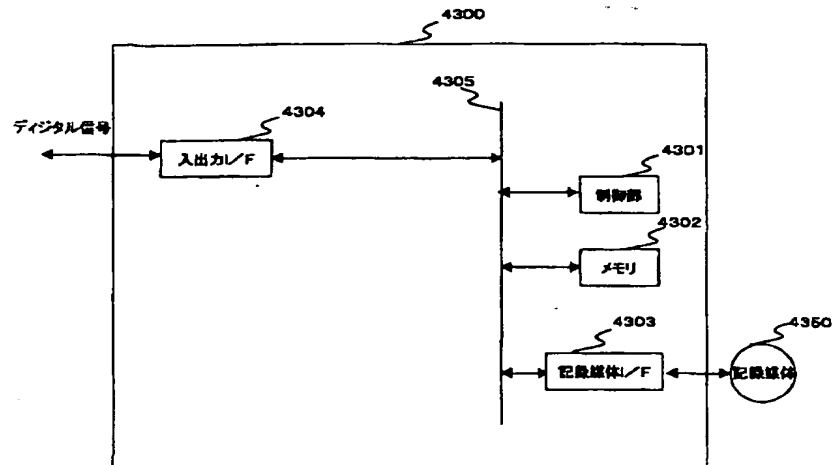
【図42】



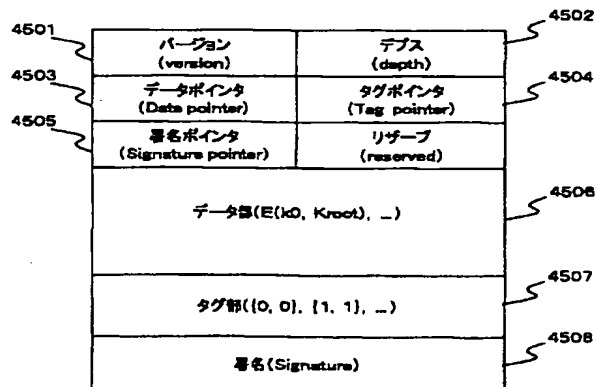
【図41】



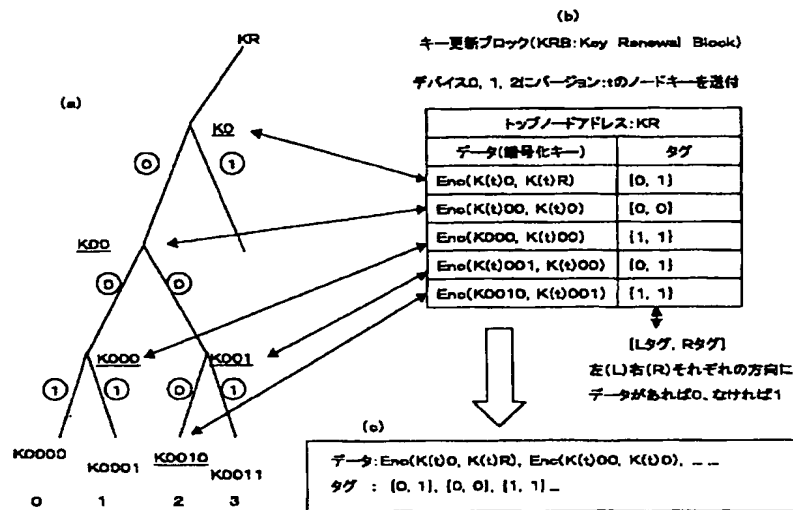
【図43】



【図45】



【図46】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

H 0 4 N 5/91

テマコード(参考)

P

(72)発明者 石黒 隆二  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72)発明者 大石 丈於  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72)発明者 光澤 敦  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

Fターム(参考) 5B017 AA06 BA07 CA09  
5C053 FA24 GB37 HA40 JA01 JA24  
JA30 KA05 KA24 KA25 LA14  
5D044 AB05 AB07 BC06 CC06 DE50  
GK17 HL02 HL08  
5J104 AA13 AA16 AA34 EA07 EA18  
EA26 NA02 NA11 NA12